Projet Sécurité
-Groupe ANALYSE-

Etudiants :

DIAGNE Aminata
PASSALACQUA Muriel
TEISSIER Benoît
ROUSSEL Jonathan
RIOTTE Nicolas
HERPIN Matthieu
ROLANDEZ Jeremy
ZERBIB Yonathan
ZERIBI Moufid

LE PLAN

Introduction

Avec le développement de l'utilisation d'Internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur Internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise.

La sécurité informatique est l'ensemble des techniques qui s'assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

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

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

La menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « *vulnerability* », appelée parfois *faille* ou *brêche*) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en oeuvre en prévention de la menace.

Les contre-mesures que nous mettrons en oeuvre ne seront pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser notre système, nous allons identifier les menaces potentielles, et essayer (tenter) de connaître et de prévoir la façon de procéder de l'ennemi (Groupe d'attaque). Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de classer ces dernières, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

Le projet : Présentation

Présentation

1-LE SUJET

Le projet consiste à étudier et à mettre en place une maquette d'infrastructure d'entreprise suivant un scénario type. Afin de mieux représenter cette maquette, 3 groupes ont été définis comme suit:

- **Le groupe d'attaque** : ce lui-ci est chargé de rechercher et de mettre en place toutes les possibilités d'intrusion et de compromission, les plus efficaces et faciles à mettre en oeuvre.
- **Le groupe défense** : celui-ci est chargé de mettre en place une infrastructure des services du scénario d'entreprise. Il doit trouver les moyens les plus simples pour se défendre contre les tentatives d'intrusion et de compromission prévues par l'attaque.
- **Le groupe d'analyse** : le nôtre, nous sommes chargés de collecter (rassembler) un maximum d'informations, de les analyser afin d'identifier les actions menées aussi bien par la défense que par l'attaque.

N.B : Notre démarche a été réalisée avec l'accord (par écrit de préférence) du plus haut niveau de la hiérarchie de « l'entreprise », c'est à dire le groupe Défense, dans la mesure où elle peut aboutir à des dégâts éventuels et étant donné que les méthodes mises en oeuvre sont interdites par la loi en l'absence de l'autorisation du propriétaire du système . Nous avons signé un engagement de responsabilité auprès du groupe Défense et de même pour le groupe Défense.
(Cf. Annexe 1 : Engagement de responsabilité).

2-Nos objectifs

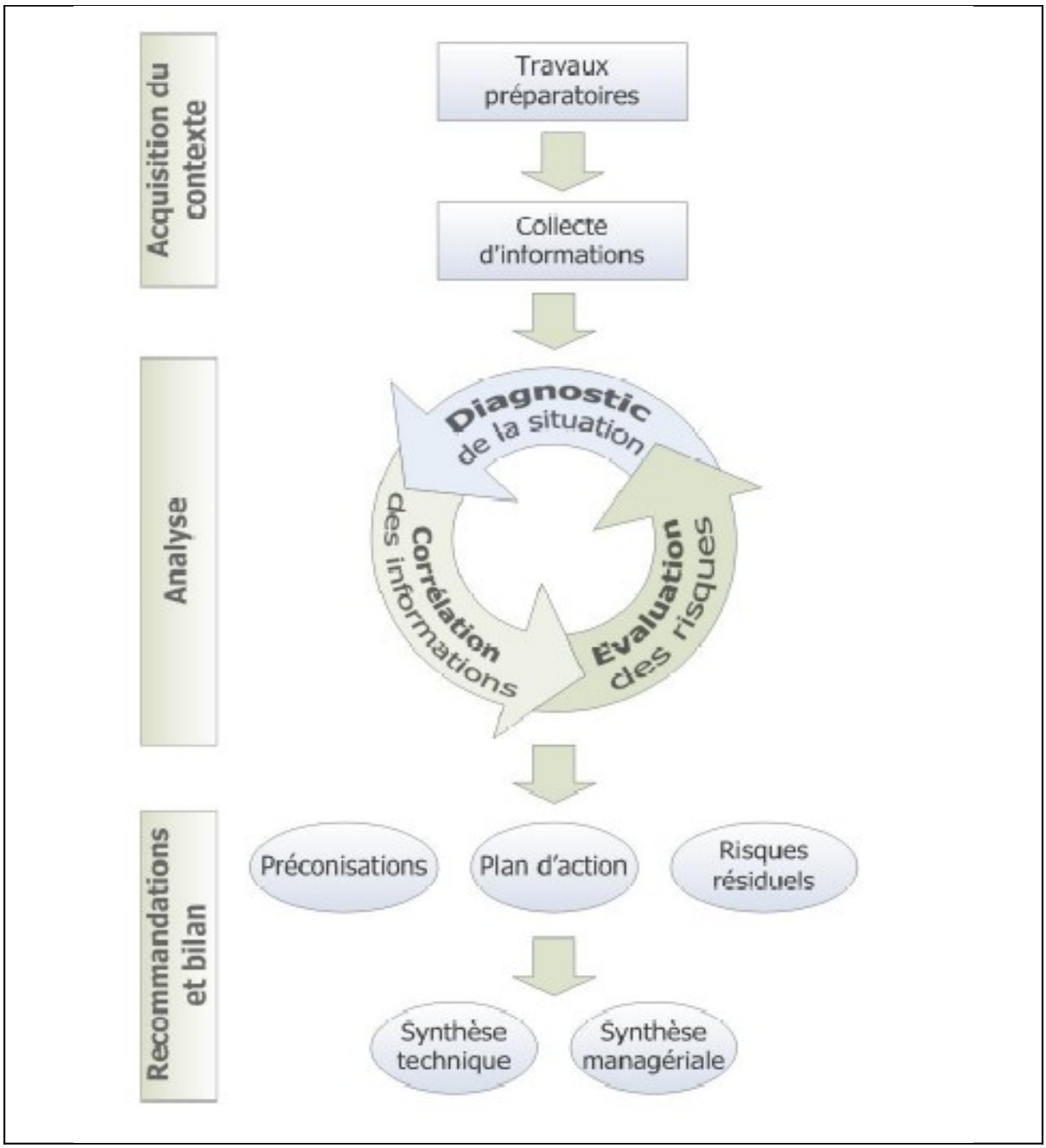
- Nous informer sur les politiques d'audit
- Anticiper et prévoir des difficultés de la sécurité informatique
- Communiquer avec les différents groupes (Défense et Attaque)
- Travailler en équipe avec une bonne coordination

3-Les buts à atteindre

Dans un premier temps, nous devons choisir une politique d'audit et la mettre en place. Ensuite, nous devons récupérer les fichiers logs contenant les informations sur le trafic réseau et repérer les attaques réussies ou en échec (précautions de l'équipe Défense). C'est la raison pour laquelle, nous avons mis en place un plan d'analyse.

Nos techniques de sécurité informatique se divisent comme suit:

- Analyse de risques
- Politique de sécurité
- Technique de sécurisation


Acquisition du contexte
Travaux préparatoires
Collecte d'informations
Analyse
Diagnostic de la situation
Evaluation des risques
Corrélation des informations
Recommandations et bilan
Préconisations
Plan d'action
Risques résiduels
Synthèse technique
Synthèse managériale

LE GROUPE ANALYSE

2.3 Présentation du groupe, Attribution des Tâches

Pour optimiser le travail au sein du groupe, nous avons constitué 3 groupes avec des tâches bien spécifiques :

Groupe 1 : Tests et évaluation du système Défense

- tests de pénétration,
- évaluation du système de défense,
- définition de la procédure reprise sur attaque, composé de *Jeremy Rolandez* et *Moufid Zeribi*.

Groupe 2 : Installation des outils

- configuration,
- installation,
- formation à l'analyse, composé de *Yonathan Zerbib* et *Mathieu Herpin*.

Groupe 3: Politique d'audit

- veille technologique,
- définition d'une politique d'audit,
- classification de la gravité des attaques via un tableau d'analyse,
- rédaction de documents officiels, composés de *Benoît Teissier*, *Muriel Passalacqua*, *Aminata Diagne*, *Nicolas Riotte* et *Jonathan Rousselle*.

N.B : Il ne s'agit pas de la première répartition du groupe, la première répartition était la suivante, mais elle n'a pas fonctionné, donc nous l'avons modifié.

Installation des machines

- **Moufid ZERIBI**: OS linux/Window
- **Yonathan ZERBIB**: OS linux

Sécurisation de notre infrastructure

- **Jeremy ROLANDEZ** (ouvertures/fermetures de ports, les combinaisons, choix du pare-feu)

Veille technologique

- **Benoît TEISSIER** : AUDITOR – WHAX
- **Johnathan ROUSSEL** : ETHEREAL – ETHERCAP – SYSLOG-NG
- **Aminata DIAGNE**: SNORT (documentations)
- **Nicolas RIOTTE** : VNC, S TUNNEL
- **Muriel PASSALACQUA**: AUDIT et coordination de l'équipe (Reporting)
- **Matthieu HERPIN** : Résumer les cours de P.LATU + MRTG (documentations)

REX : cette répartition n'a pas fonctionné car il y avait un manque d'écoute et un gros problème de communication. Les personnes ne suivaient pas leurs rôles au point d'effectuer des tâches et des rôles attribués à d'autres personnes.

L'individualisme de certaines personnes dans leur manière de travailler a posé problème car ces personnes fonçaient têtes baissées dans la technique avant même d'envisager de mettre en place une méthode d'analyse (Process). Résultat, aucune structure, tout le monde partait dans tous les sens sans aucune écoute. Très difficile pour la personne qui coordonnait l'équipe. Après plusieurs tentatives d'écoute, la communication était toujours unidirectionnelle. Alors, elle a baissé les bras en cédant sa place et s'en effaçant. Cette phase a démotivé certains membres de l'équipe qui ne se sentaient pas écoutés.

2.4 Objectifs Pédagogiques

Dans la plupart des projets, le principal objectif est technique : faire prendre conscience aux étudiants de l'intérêt du sujet en milieu informatique professionnel et de sa complexité intrinsèque. Tout ceci afin d'étayer les cours magistraux.
Ici, l'aspect technique a déjà été abordé lors des années de formation précédentes. Il restait cependant à « tester » les étudiants lorsque l'ensemble du projet est en leur entière responsabilité.
C'est donc plutôt la gestion de projet et la communication entre groupes, voir entre membres du même groupe, qui était mise à l'épreuve.
Les étudiants devaient pour se faire endosser leur rôle de façon fidèle. Ainsi le groupe défense, dans son optique sécuritaire, a tâché de ne distribuer les informations sur le réseau de l'entreprise Candide SA qu'au compte-goutte, y compris au groupe analyse, et ces deux groupes devaient autant que possible éviter la communication avec le groupe d'attaque.
Le but étant bien entendu de laisser s'exprimer les inévitables frictions. On peut avancer l'hypothèse qu'une fois ces problèmes de communication clairement mis en lumière, les étudiants auront à cœur d'y remédier dans leur travail en entreprise.

Le Métier d'Analyste

3.4Politique Sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Elle doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle nous pensons qu'il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en oeuvre se fait selon les quatre étapes suivantes :

1- **Identifier les besoins** en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

Cette phase consiste dans un premier temps à **faire l'inventaire du système** d'information, notamment pour les éléments suivants :

- Personnes et fonctions ;
- Matériels, serveurs et les services qu'ils délivrent ;
- Cartographie du réseau (plan d'adressage, topologie physique, topologie logique, etc.) ;
- Liste des noms de domaine de l'entreprise ;
- Infrastructure de communication (routeurs, commutateurs, etc.) ;
- Données sensibles.

2- **Elaborer des règles et des procédures** à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés ;

L'étape d'analyse des risques consiste à **répertorier les différents risques** encourus, d'estimer leur probabilité et enfin d'étudier leur impact.

La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait (par exemple attaque sur un serveur ou détérioration de données vitales pour l'entreprise).

Sur cette base, il peut être intéressant de dresser un **tableau des risques** et de leur **potentialité**, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonné selon un barème à définir, par exemple :

- Sans objet (ou improbable) : la menace n'a pas lieu d'être ;
- Faible : la menace a peu de chance de se produire ;
- Moyenne : la menace est réelle ;
- Haute : la menace a de grandes chances de se produire.

3- **Surveiller et détecter les vulnérabilités** du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

4- **Définir les actions à entreprendre** et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations que nous avons suivies (à prendre au sens large) en terme de sécurité.

Elle représente le **document de référence** définissant :

- les objectifs poursuivis en matière de sécurité,
- les moyens mis en oeuvre pour les assurer,
- un certain nombre de règles, de procédures,
- et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Ce document sera conduit comme un véritable projet. La phase de mise en oeuvre consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité.

Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont les **systèmes pare-feu**. Néanmoins ce type de dispositif **ne protège pas la confidentialité** des données circulant sur le réseau.

Nous avons mis en place un système de tunnels sécurisés (**VPN** : **V**irtual **P**rivate **N**etwork) pour nous permettre d'obtenir un niveau de sécurisation supplémentaire dans la mesure où l'ensemble de la communication est chiffrée.

3.5Audit de Sécurité

L'audit de sécurité est souvent négligé au profit de simples tests d'intrusion ou de vulnérabilité. Il est pourtant le préalable à toute vraie démarche de sécurisation. Il est une **vue interne du système** d'information qu'il ne faut pas confondre avec des tests externes.

L'audit de sécurité (en anglais *security audit*) consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre par le groupe Défense, au regard de la politique de sécurité. Notre objectif est de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent. Cela nous permettra de nous assurer que l'ensemble des dispositions prises par « le groupe Défense » sont réputées sûres.

Deux types d'audits se complètent, plus qu'ils ne s'opposent. Un **audit formel** commence par une analyse de l'organisation et se termine par des **recommandations**. Entre les deux, un projet parfois long et complexe et qui implique toute l'entreprise.

Comment préparer notre audit ?

Pour que notre audit fonctionne bien, il nous faut une implication hiérarchique forte, de préférence au niveau du groupe Défense. Il faut aussi que les personnes concernées (administrateurs des machines, services informatiques) soient impliqués dès le départ.

Quelles sont les informations nécessaires ?

Un audit n'est pas seulement basé sur des informations techniques. Il nous faut des procédures :

- Quand sont faites les sauvegardes ?
- Comment sont suivies les machines ?
- Une veille technologique en matière de sécurité est-elle mise en place?
- Etc…

C'est pourquoi, il faut impliquer tout le monde et pas seulement les techniciens !!!

Combien de temps prend un audit ?

C'est très variable (3 jours, une semaine, 15 jours), mais la discussion est importante pour préparer convenablement un premier audit. On peut certes envisager des interventions plus rapides, sous la forme d'audits " coup de poing " afin de sanctionner la non application de consignes préalables. Mais ce n'est jamais agréable pour l'auditeur, et heureusement, on n'en a pas fait.

Nous avons consacré d'ailleurs du temps à expliquer notre démarche et à travailler à l'amélioration du système. Passé le premier audit, les suivants ont été plus rapides. Ils demeurent nécessaires car il s'agit d' un processus et non d'une prestation unique !

3.6Méthode d'Audit

A- Méthode d'audit suivie

Notre méthode fonctionne en 3 phases. Nous avons souhaité auditer :

- Les vulnérabilités,
- l'identification des points faibles de la politique de sécurité. En découle une analyse des risques (distinction entre risques majeurs et simples),
- et, une mise en avant des menaces potentielles. Partant de là (3e phase), des plans d'action sont définis.

L'audit de vulnérabilité nous permet d'adopter une approche automatisée et exhaustive des tests de sécurité. En aucun cas il remplace le test d'intrusion qui lui intervient en amont de tout projet sécurité car il permet de déceler des faiblesses sur les architectures. De plus, le test d'intrusion nous permet également de sensibiliser la direction aux problématiques sécurité et aide dans bien des cas à obtenir des budgets pour la sécurité. Il possède une approche plus régulière que le test d'intrusion, il doit nous permettre de mesurer le niveau de sécurité et de contrôler l'imperméabilité du réseau. Dans le cas ou les résultats ne sont pas satisfaisants, l'audit de vulnérabilités doit nous conduire à un processus de remediation des vulnérabilités découvertes.

La qualité d'une solution d'audits de vulnérabilités réside dans plusieurs facteurs:

- La taille et la fréquence de mise à jour de la base de connaissances.
- La précision de la détection des vulnérabilités notamment face aux problématique des faux positifs ou faux négatifs.
- La capacité de la solution à extraire des rapports détaillés et exploitables pour des techniciens.
- La capacité de la solution à s'adapter à l'entreprise notamment face aux problématiques de centralisation de la gestion de la solution et aux problématique d'entreprises multi-sites.

B- Méthode d'audit : Les phases

Un audit de vulnérabilités se déroule généralement en quatre phases. Ces phases sont les piliers de la démarche proactive de gestion de vulnérabilités.

1-Phase de découverte

La première phase dite de vulnérabilités est la découverte des machines à auditer. Nous avons besoin de connaître avec précision son périmètre réseau aussi bien interne que externe. Certaines solutions offrent des fonctionnalités de mapping qui permet d'effectuer un inventaire du parc interne ou externe et de choisir les machines à tester. Évidemment les machines dites "*sensibles*" sont les premières à auditer mais il ne faut pas néanmoins que nous négligeons les autres y compris les stations de travail qui, nous l'avons vu avec l'arriver de vers comme "*sasser*" ou "*blaster*", sont des cibles de choix pour les développeurs de virus.

2-Phase de détection

La phase de détection ou "Assessment" correspond à la détection des vulnérabilités présentes sur les machines testées. Nous devons opéré cette phase de manière récurrente et automatisée. A partir de la base de connaissance de la solution d'audits, celle-ci va nous permettre de déterminer les vulnérabilités présentes sur une ou plusieurs machines ou éléments actifs. En fonction de la solution utilisée, cette phase peut être plus ou moins intrusive. Certains éditeurs de solutions d'audit de vulnérabilités adoptent une politique "*non intrusive*" afin de pouvoir tester sans risques des serveurs en production.

3-Phase d'analyse des résultats

Cette phase correspond à l'exploitation des résultats de la phase de test. La solution d'audits de vulnérabilités nous sera à même de nous fournir un reporting précis, détaillant les problèmes rencontrés, l'impact sur les machines et les solutions pour corriger les failles. Certaines solutions nous offrent également des rapport dits "Exécutive" qui n'étant pas techniques, s'adressent plus aux personnes faisant un état des lieux du niveau de sécurité global du système informatique et fournis également des rapports d'analyse de tendance sur une période donnée. Cela permettra au groupe Défense de visualiser l'efficacité de leurs équipes sécurité et de pouvoir visualiser leurs retours sur investissements dans le domaine de la protection de l'infrastructure informatique.

4-Phase de remédiation

Cette dernière phase a pour but de gérer au mieux les interventions qui font suite aux découvertes. Certaines solutions d'audits de vulnérabilités fournissent une plateforme d'attribution de ticket lors de la découverte d'une vulnérabilité. Le ticket adressé à un technicien lui permet de mettre en place une action curative et de tracer les événements de remediation. Le processus de remediation doit être l'aboutissement d'un audit de vulnérabilités.

Conclusion : L'audit de vulnérabilité récurrent est donc un point clé de la sécurité d'un système d'information. Il nous a permis de maintenir un niveau de sécurité et de prévenir les attaques et intrusions. Sa démarche a été proactive. Contrairement à la détection d'intrusion qui a adopte une démarche passive, l'audit de vulnérabilité récurrent nous a permis de détecter au plus vite et avant incident une ou plusieurs vulnérabilités qui auraient pu être exploités par un vers ou un pirate informatique.

Les Outils utilisés – Les résultats

5.8Sondes utilisées, Choix des OS

Après plusieurs tests sur des OS différents, nous avons décider d'opter pour un OS fiable et que nous connaissions bien : Linux DEBIAN.
En effet, les tests que nous avons effectué se sont portés sur des distributions en Live CD, autrement dit, des distributions qui démarrent sans installation préalable. Le problème que nous avons rencontré lors de ces tests est le fait qu'aucune des distributions ne convenaient pleinement à notre cahier des charges. De plus, ces distributions chargent au démarrage des applications qui n'étaient pas souhaitées. Nous ne pouvions pas nous permettre d'installer n'importe quoi sur ces sondes car elles sont intégrées dans le réseaux « défense » et donc elle ne doivent en aucun cas affaiblir le périmètre que nous souhaitons évaluer.
L'avantage de ces distributions c'est qu'elles sont de nouveau opérationnelles après un simple reboot.
L'OS Linux Debian a été choisi pour différentes raisons. La première et la plus importante est que nous l'avons utilisé et même pratiqué depuis assez longtemps pour en avoir une maîtrise suffisante pour ce projet.
Cet OS offre de plus une importante modularité. En effet, une fois le noyau installé sur la machine, il est possible d'orienter l'OS au maximum est n'installer que le strict nécessaire au projet en cours.
Linux Debian contient également un utilitaire très intéressant en ce qui concerne la gestion des paquets. Il est donc très simple d'installer une application car le système s'occupe alors de gérer toutes les dépendances aux paquets souhaités.

5.9Services utilisés

Les services installés sur la machine ont été rapportés au minimum. La sonde se comporte comme un serveur de données. En effet, elle ne servira qu'à récupérer ou générer des informations sur le trafic du réseau. Ces données seront accessibles via un serveur WEB.

Sur cette machine il y aura donc les services suivants :

- Un serveur Apache
- Un serveur OpenVPN : nécessaire pour l'accès à distance aux machines
- Un daemon SSH : Pour crypter les communications issue du VPN
- Un daemon MySQL : nécessaire pour la récupération et l'archivage des données

5.10Snort/AcidLab

5.10.1Snort

On ne présente plus Snort, le fameux système de détection d'intrusion réseau (NIDS) de la communauté Open Source. Bien que ce logiciel possède 3 fonctions, dont celle de sniffer réseau, nous ne nous intéressons qu'à la principale : la détection d'intrusion.
Cette fonction, comme son nom l'indique, ne fais pas concurrence au pare-feu, mais prévient l'administrateur lorsqu'une tentative d'intrusion du réseau à été détectée. La méthode d'inspection utilise des règles combinant signature, protocole et utilisation anormale. Un des points forts de Snort est que le format de ces règles est devenu un standard de fait dans l'industrie des IDS (voir des firewalls). Lors de l'installation, 1200 règles environ sont pré-configurées. Moyennant une somme forfaitaire, il est possible d'acquérir un ensemble de presque 5000 règles rédigées par des spécialistes (Sourcefire), couvrant la majorité des attaques possibles. Les règles ne sont pas tout, encore faut-il savoir où positionner l'IDS.
La méthode la plus répandue consiste à brancher une machine linux en mode *stealth* (furtif – l'interface reçoit les paquets mais n'en émet pas) sur un nœud du réseau (typiquement un Hub afin de recevoir l'ensemble des paquets transitant sur ce segment du réseau). Pour le groupe Analyse, le but étant de tester l'efficacité des systèmes de prévention de la défense, il est intéressant de mettre une sonde en amont et une autre en aval du pare-feu, dans le domaine des services notamment.

Reste alors à analyser les logs de Snort. En mode console, les experts joueront du *grep* et du *find*, nous, simples étudiants, avons choisi une interface graphique dédiée, développée par une autre équipe, appelée AcidLab.

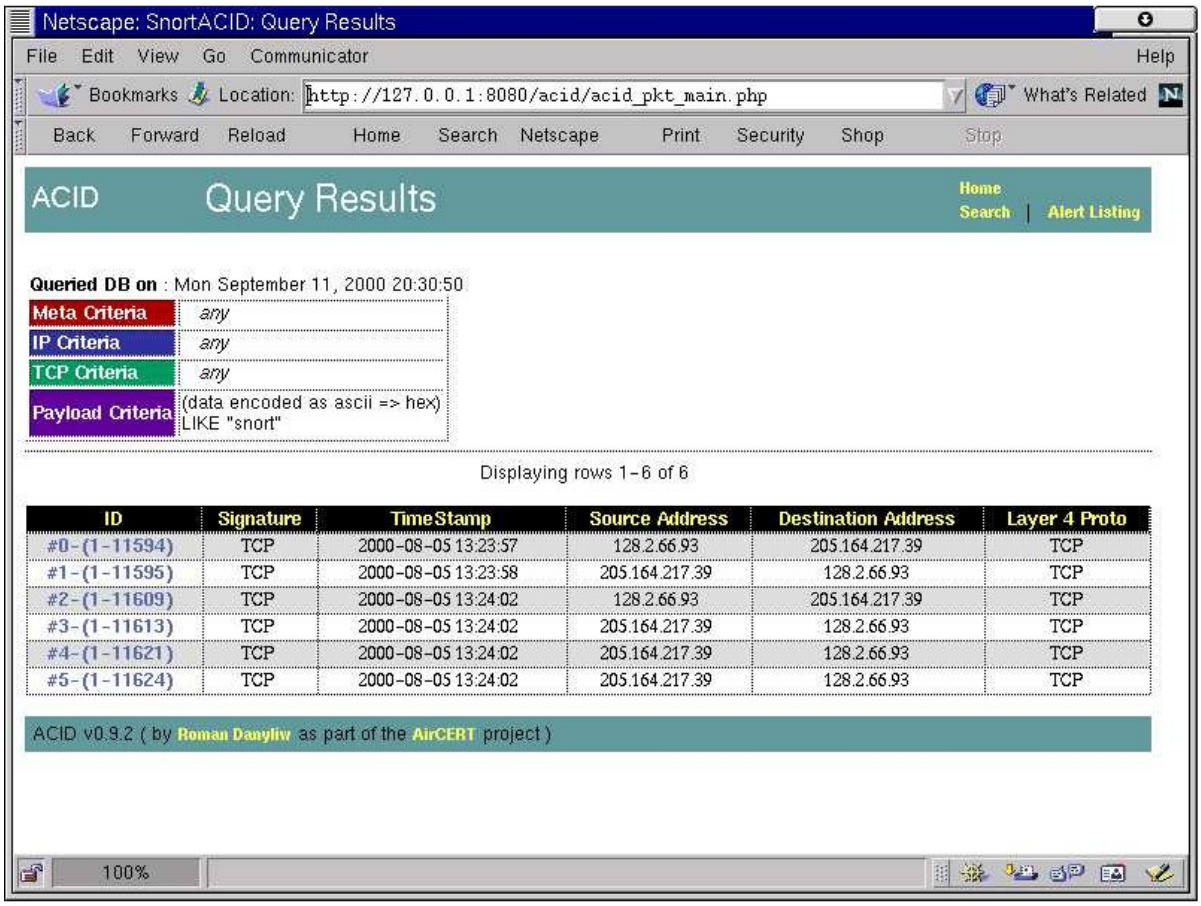
5.10.2AcidLab

Cette interface graphique, également Open Source, n'est pas implémentée directement sur la sonde (heureusement). Il s'agit en réalité d'une interface Web, écrite en PHP, qui utilisera les données enregistrées par Snort dans une base SQL (MySQL dans notre cas) afin de générer dynamiquement des comptes-rendus. Il nous a donc fallu abandonner le mode stealth afin d'accéder au serveur web.

AcidLab (pour Analysis Console for Intrusion Databases) possède 4 fonctions :

- Interface de recherche (Query Builder)
- Analyse de paquets
- Management des alertes
- Génération de statistiques

On peut bien sûr trier les résultats en fonction d'un champ particulier.



Exemple de présentation d'information par AcidLab

5.11TEthereal/Ethereal

TEthereal est un analyseur de trafic réseau Open Source. On l'utilise afin de générer des statistiques des données transitant sur le réseau, ou par exemple en sécurité pour analyser de façon détaillée une session entre deux machines.
Il est possible de l'alimenter en le connectant directement sur le réseau (comme pour Snort, le mode *stealth* derrière un hub est conseillé) et en lançant une capture *live*, ou en lui ordonnant d'analyser un fichier de capture, généré par exemple par tcpdump ou Snort en mode sniffer.

Pour affiner l'analyse du trafic, on peut implémenter des règles de filtrage lors de la capture, en fonction

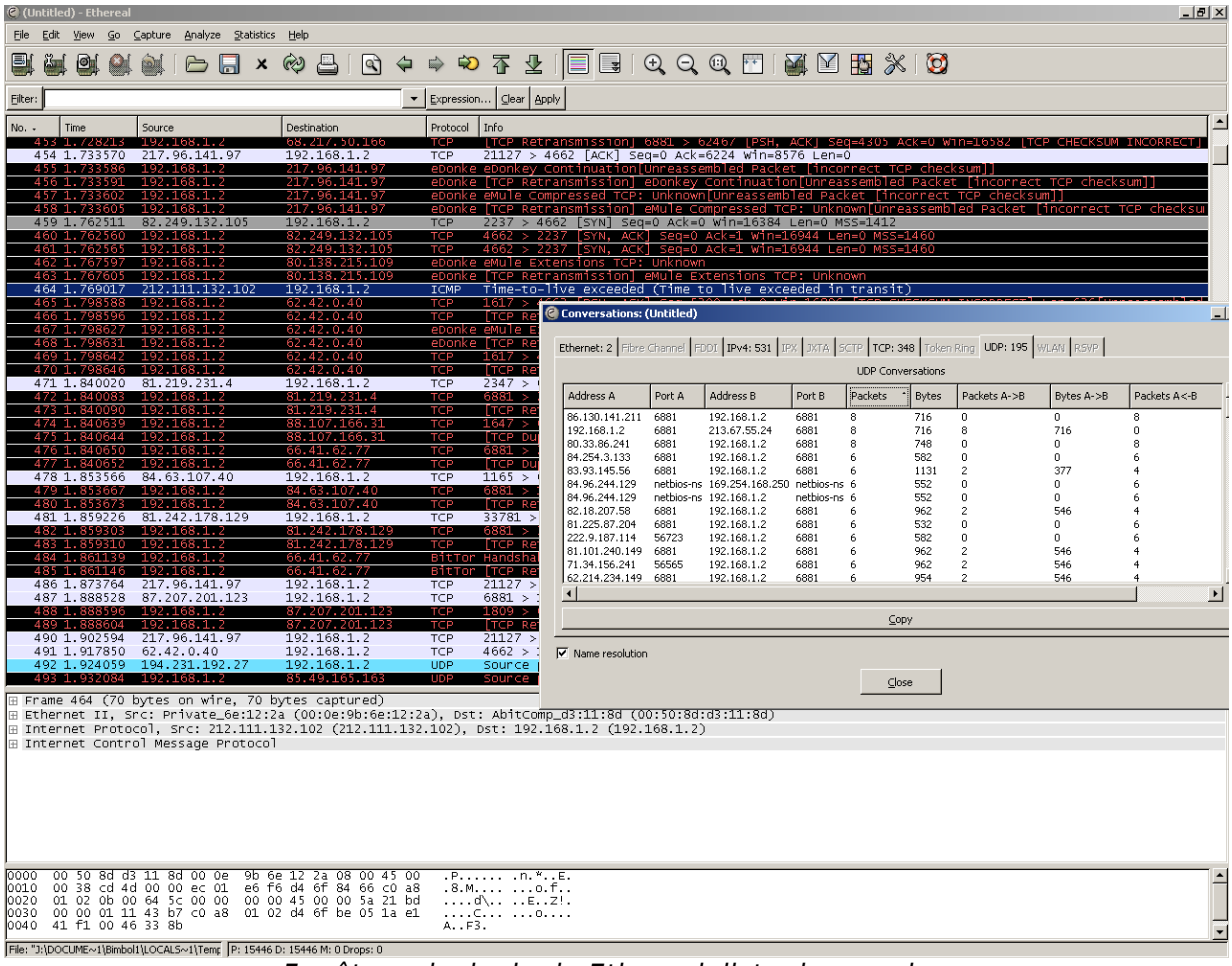
- Du protocole
- De la direction
- D'un champs de paquet.

On peut combiner les filtres avec les opérateurs AND, OR et NOT.

Il est également possible de filtrer l'affichage. Les règles sont différentes de celles dédiées à la capture, car plus complètes. On peut détailler chaque champ, et utiliser un plus grand nombre d'opérateurs.

La génération de statistiques est bien sûr une fonction très intéressante de TEthereal. On peut ainsi visualiser en un clin d'œil la source d'un trafic anormal, et avant cela détecter ce trafic.

Comme pour Snort, nous avons choisi d'utiliser une interface graphique. Elle est intégrée à TEthereal et s'appelle… Ethereal. Le tri par champ est une fonctionnalité plus qu'utile.



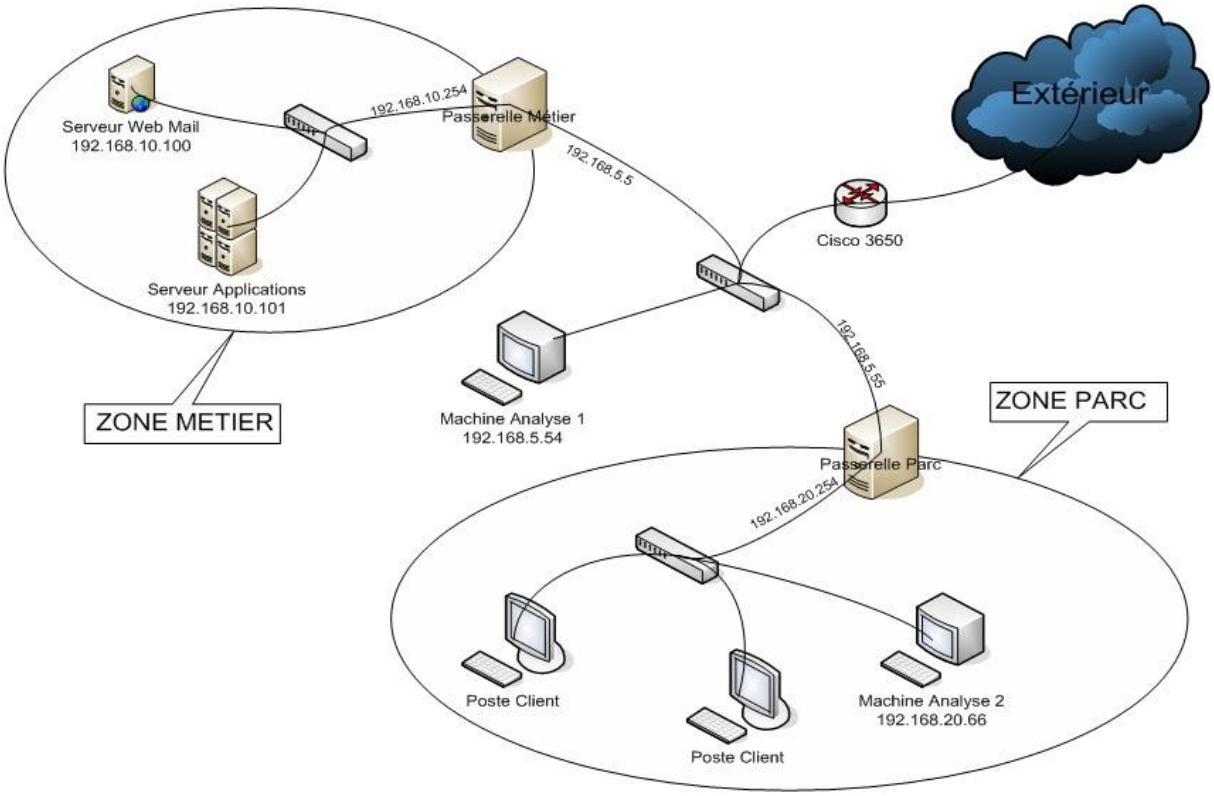
Fenêtre principale de Ethereal, liste des sessions.

5.12OpenVPN

Ici nous allons parler de l'infrastructure mise en place.
Nous avons placé une machine en dehors du périmètre réseau. Je nommerai cette machine comme étant à l'extérieur du périmètre de service, ceci par abus de langage.
Conformément avec l'équipe de gestion du réseau (équipe Défense) de l'entreprise Candide SA, nous avons récupérer une adresse IP à attribuer à cette machine : **192.168.5.54**

Nous avons également placé une machine à l'intérieur du réseau. Nous nous sommes également mis d'accord avec l'équipe Défense pour récupérer une adresse IP à cette machine : **192.168.20.66**

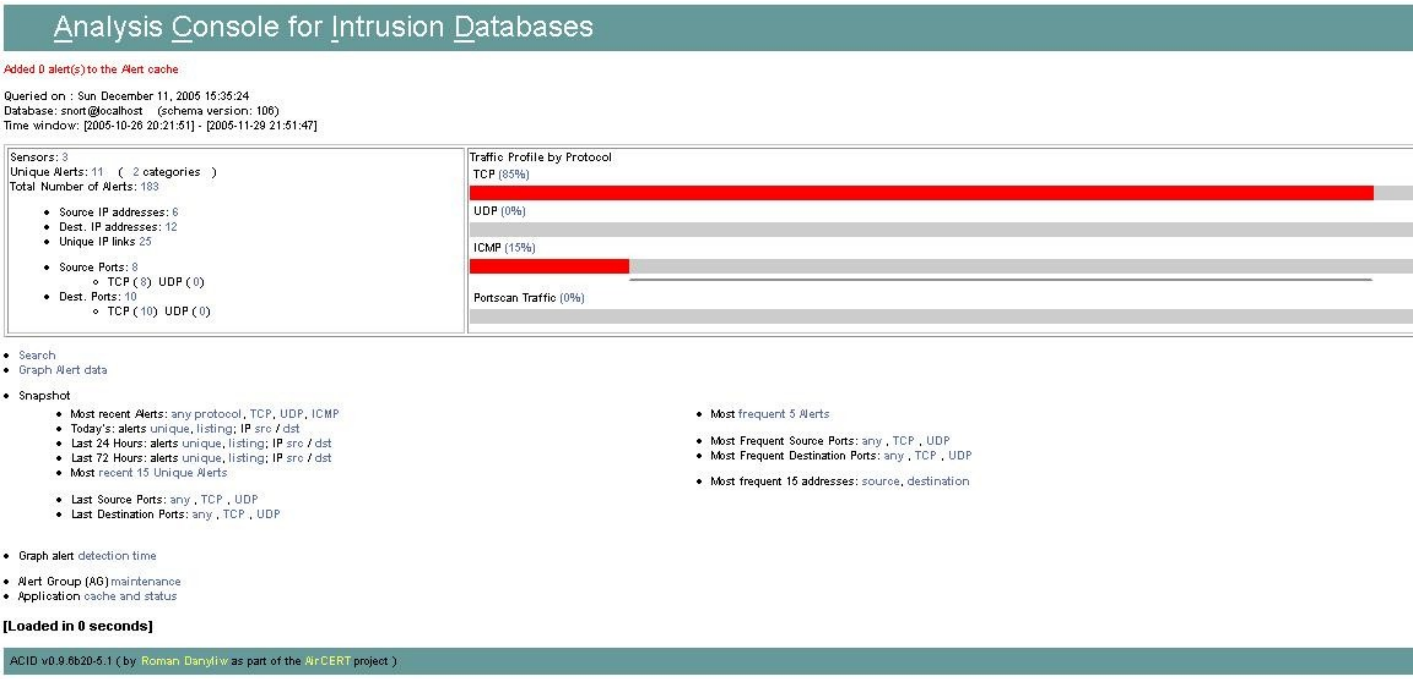
En effet nous avions à notre disposition deux machines.
Sans redéfinir les différents choix que nous pris, voici l'infrastructure du réseau de l'entreprise Candide S.A.



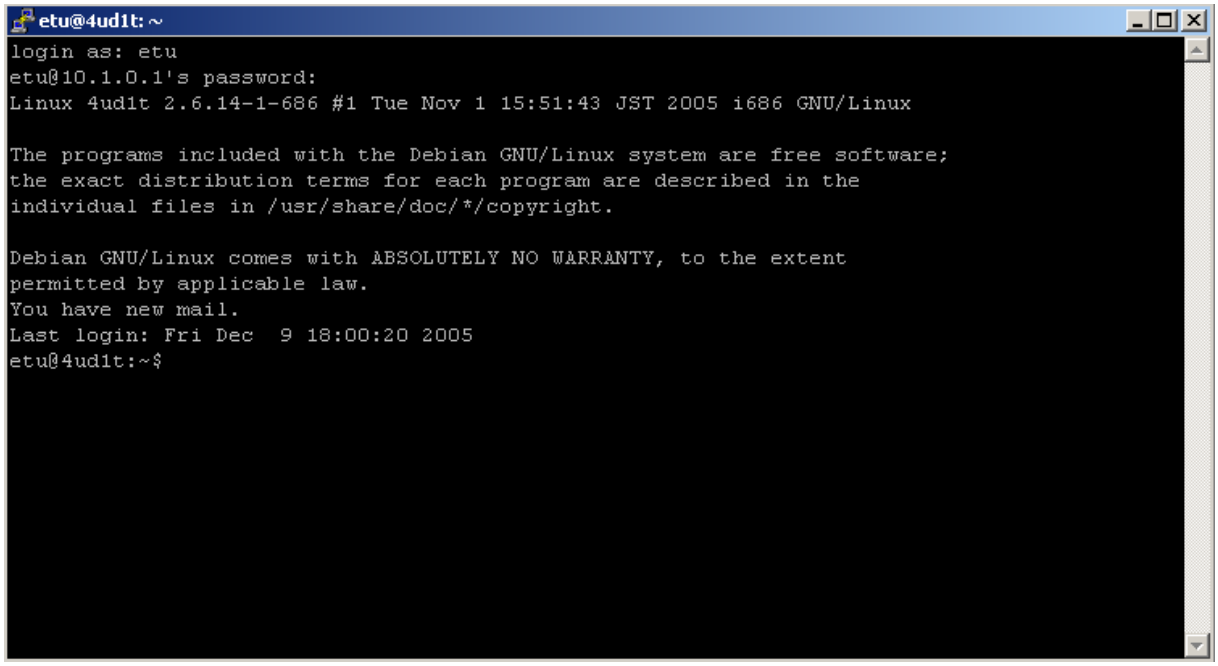
Pour accéder aux machines, nous avons également mis en place quatre tunnels VPN (deux par machines).

Pour nous connecter aux machines et aux références d'intrusion de ACID Lab, nous avons utilisé OpenVPN :

Voici un exemple de compte rendu de ACIDLab :



Nous avons également utilisé Putty, pour nous loger en SSH sur les machines afin de pouvoir les manipuler à distance :



5.13Nmap

Le but est de fournir un reporting au groupe défense concernant un audit du système.
L'audit comprend 2 étapes. La première est un audit interne en définissant le périmètre d'intervention.
Le deuxième concernant un audit sur l'extérieur, c'est-à-dire le nuage Internet.

Nous devons planifier l'analyse, définir quels sont les points techniques à développer, quels vont être les outils pour aboutir. SNORT, MySQL, ACID…
Nous devons également estimer le temps et l'effort pour une procédure d'analyse.
Les risques d'une mauvaise analyse doivent être également pris en compte.

Nous devons également analyser le périmètre défense et faire des recommandations d'améliorations ou d'architectures alternatives.
Le risque d'attaque suit donc la relation suivante :

Risque = Menace x Vulnérabilité

D'où la nécessité de savoir la vulnérabilité des systèmes engendrés dans le système.
Pour cela nous avons procédé à une découverture du réseau interne. Les outils utilisés afin de découvrir le réseau ont été principalement des scanners de ports comme Nmap. Pourquoi les scanners de ports sont-ils si importants au sein d'un réseau ? Fondamentalement parce que ce sont des outils indispensables à ceux qui souhaitent attaquer un système. Les différentes méthodes pour la préparation d'une attaque sont les suivantes :

- scanner une machine ou un réseau, observer les services en cours et les systèmes qui les exécutent et s'appuyer sur les vulnérabilités connues de ces services ou de ces systèmes.
- scanner une machine ou un réseau à la recherche d'un service ou d'un système particulier (incluant la vérification de la version) dont la vulnérabilité est connue.

Pour cette raison, nous avons scanné le réseau afin d'y chercher les points faibles avant que d'autres, aux intentions moins avouables, ne s'en chargent.

Nmap offre plusieurs techniques de "balayage".Le résultat affiché par nmap est généralement une liste des ports "intéressants" (les ports actifs) sur la machine scannée. Pour chacun de ces ports il fournit le nom du service connu, l'état et le protocole.

```
C:\Documents and Settings\Kiki>nmap
Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

Balayage utilisant le"three way handshake" de TCP (option -sT)

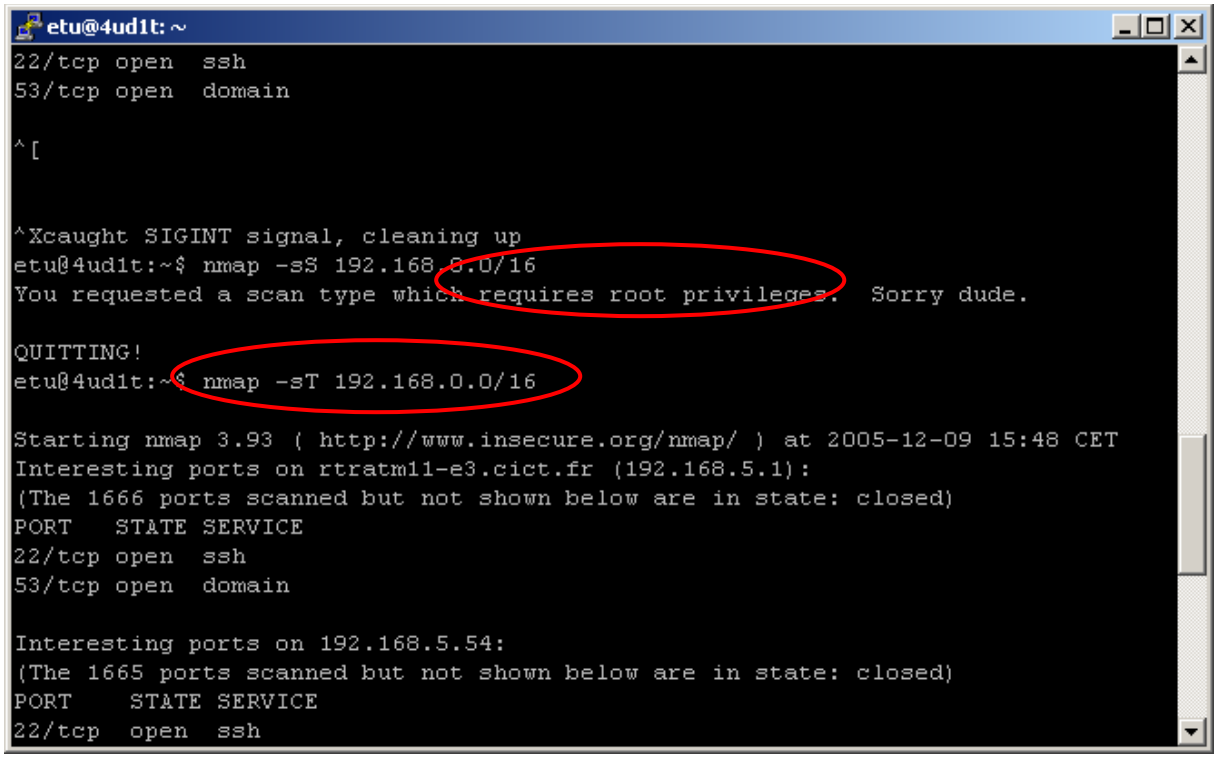
La forme de scan la plus commune consiste à utiliser l'option -sT. Ce mode se base sur l'établissement de la connexion par TCP, plus connu sous le nom de "three way handshake".

a) Le serveur doit être prêt à recevoir une connexion (en général, en utilisant les fonctions socket, bind et listen).

b) Le client lance une connexion active - il appelle connect() - Il envoie un segment SYN pour informer le serveur du numéro initial de séquence pour les données que le client va envoyer sur cette connexion. Normalement, SYN contient un Header (entête) IP - un Header TCP et peut être une option TCP.

c) Le serveur doit informer de la reconnaissance le SYN en envoyant un ACK, et à son tour envoie un SYN avec son numéro de séquence (le tout en un seul paquet TCP).

d) Le client doit informer de sa reconnaissance le SYN envoyé par un ACK.
Ce mode de balayage a deux avantages :
il n'est pas nécessaire d'avoir des privilèges particuliers pour l'exécuter sur la machine qui le lance et il a le gros inconvénient d'être très simple à détecter et facile à filtrer.



Balayage utilisant les segments SYN (à demi ouvert - half open - option -sS)

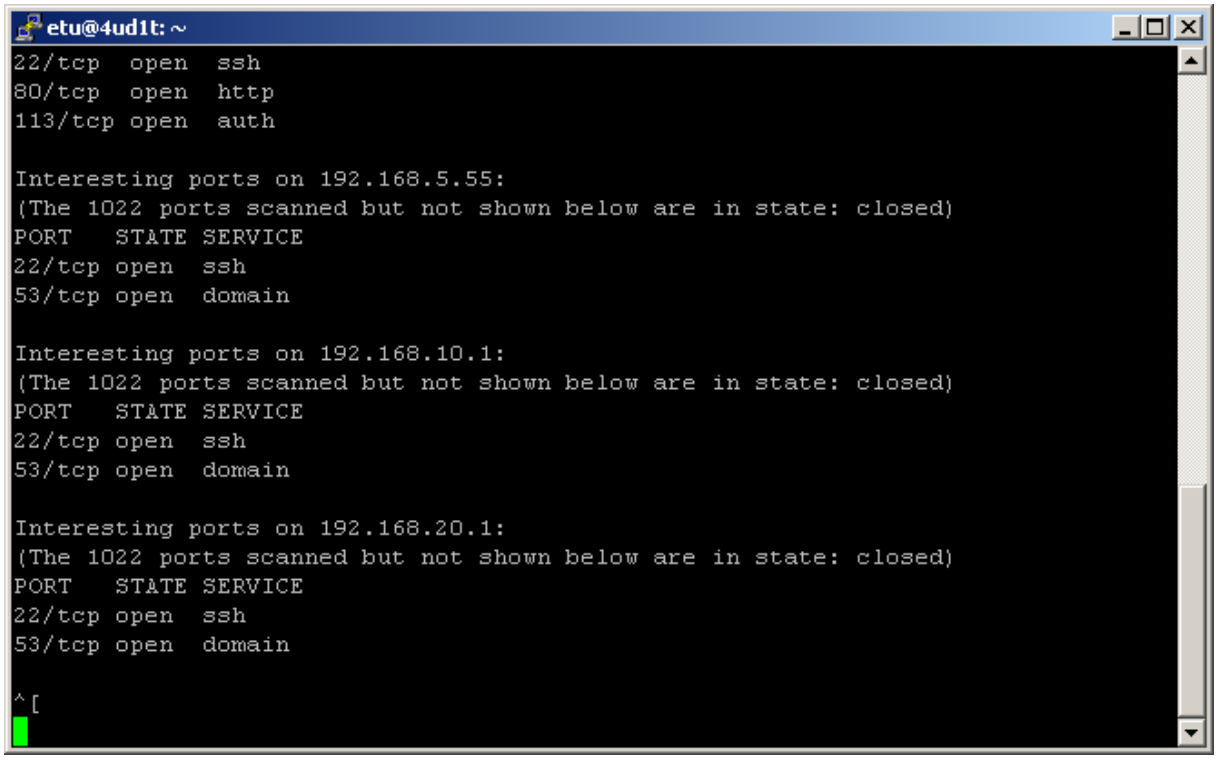
Ce type de balayage s'obtient en exécutant nmap avec l'option -sS. La technique utilisée consiste à ouvrir une "demi-connexion", c'est-à-dire à envoyer un segment SYN et si un ACK est reçu c'est parce qu'un port actif a été détecté sur la machine cible, à la suite duquel un RESET est envoyé pour couper brutalement la communication. Si un RST est reçu à la place d'un ACK c'est que le port de la machine cible est inactif. Ce type de scan a pour inconvénient de nécessiter les privilèges de root. Par contre il offre l'avantage d'être **difficile à détecter sur la machine visée.**

Voici la détection par SNORT d'un scannage de port, certainement avec nmap.

[snort] (portscan) Open Port	2005-11-29 10:07:33	192.168.5.2	192.168.10.10
[snort] (portscan) Open Port	2005-11-29 10:07:33	192.168.5.2	192.168.10.10
[snort] (portscan) TCP Portscan	2005-11-29 10:07:33	192.168.5.2	192.168.10.10
[snort] (portscan) Open Port	2005-11-27 14:03:29	192.168.10.254	192.168.10.10
[snort] (portscan) Open Port	2005-11-27 14:03:29	192.168.10.254	192.168.10.10
[snort] (portscan) Open Port	2005-11-27 14:03:29	192.168.10.254	192.168.10.10
[snort] (portscan) TCP Portscan	2005-11-27 14:03:29	192.168.10.254	192.168.10.10
[snort] (portscan) Open Port	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) Open Port	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) Open Port	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) Open Port	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) Open Port	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) TCP Portscan	2005-11-27 14:01:08	192.168.10.254	192.168.10.2
[snort] (portscan) TCP Portsweep	2005-11-27 14:01:08	192.168.10.254	192.168.10.2

Nous avons également utilisés l'option – p <range>

Ex : nmap –p 1-1024 192.168.0.0/16



Voici la configuration du réseau que nous avons scanné en date du **25/11/2005** ainsi que les différents ports ouverts et les daemons tournant sur les différentes stations.

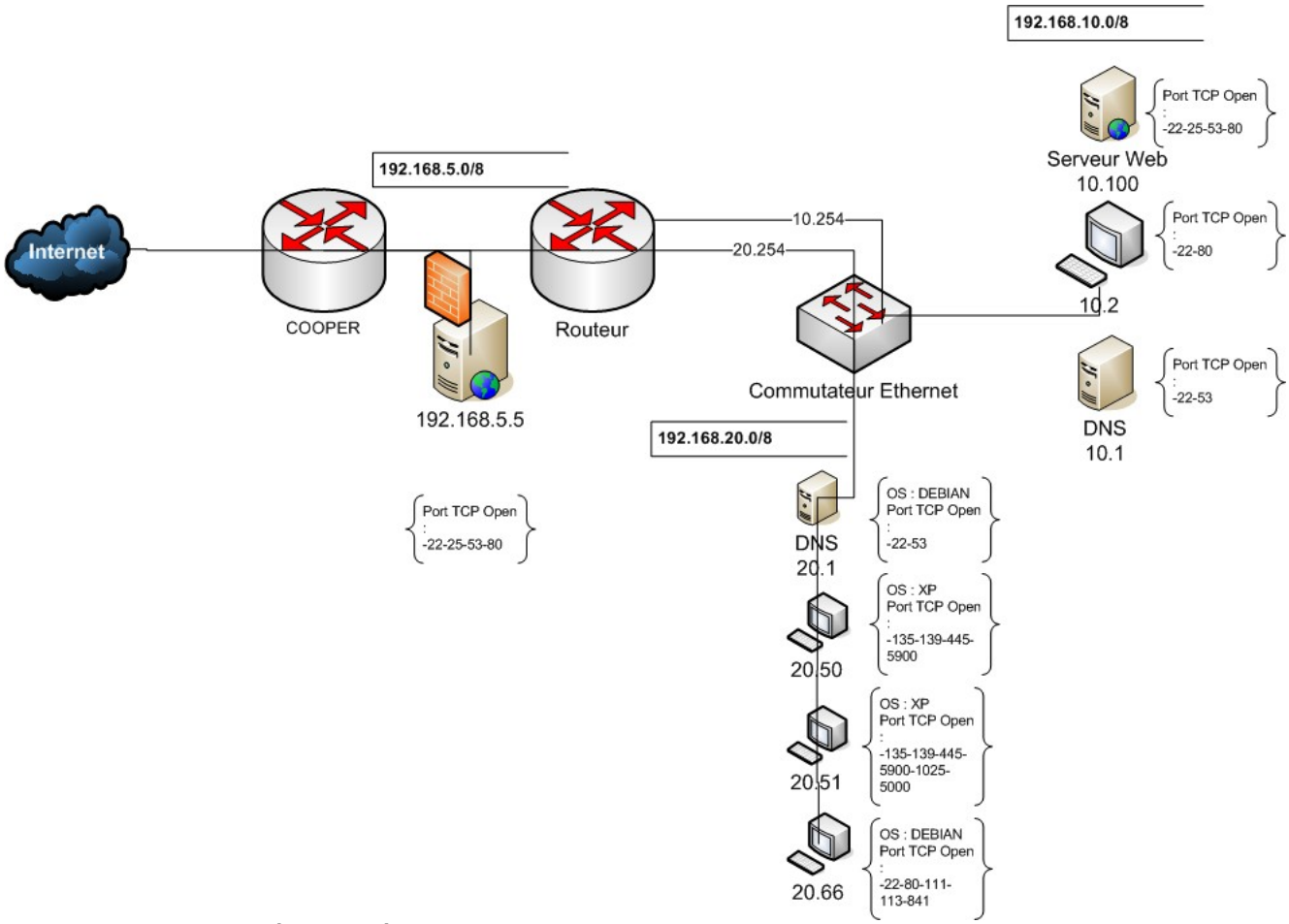


Figure 1 - Map du réseau découvert le 25/11/05

5.14Nessus

Afin de réaliser un Audit complet du réseau, nous avons également mis en place de tests de sécurité à l'aide de l'outil *Nessus.*

Mais qu'est ce que Nessus ?

Ici aucun rapport avec la mythologie Greque ! (Pour rappel : ***Nessus***, *centaure qui, ayant voulu enlever Déjanire, femme d'Hercule, fut atteint par le héros d'une flèche trempée dans le sang de l'hydre de Lerne. En mourant Nessus donna sa tunique à Déjanire comme un talisman qui devait lui ramener son époux, s'il devenait infidèle. Hercule, lorsqu'il l'eut revêtue, en fut consumé.*)

Nessus est un outil de sécurité permettant de scanner une ou plusieurs machines. Il permet aussi de tester différentes attaques pour savoir si une ou plusieurs machines sont vulnérables.

Il est très utile lors de tests de pénétration et fait gagner un temps incroyable.

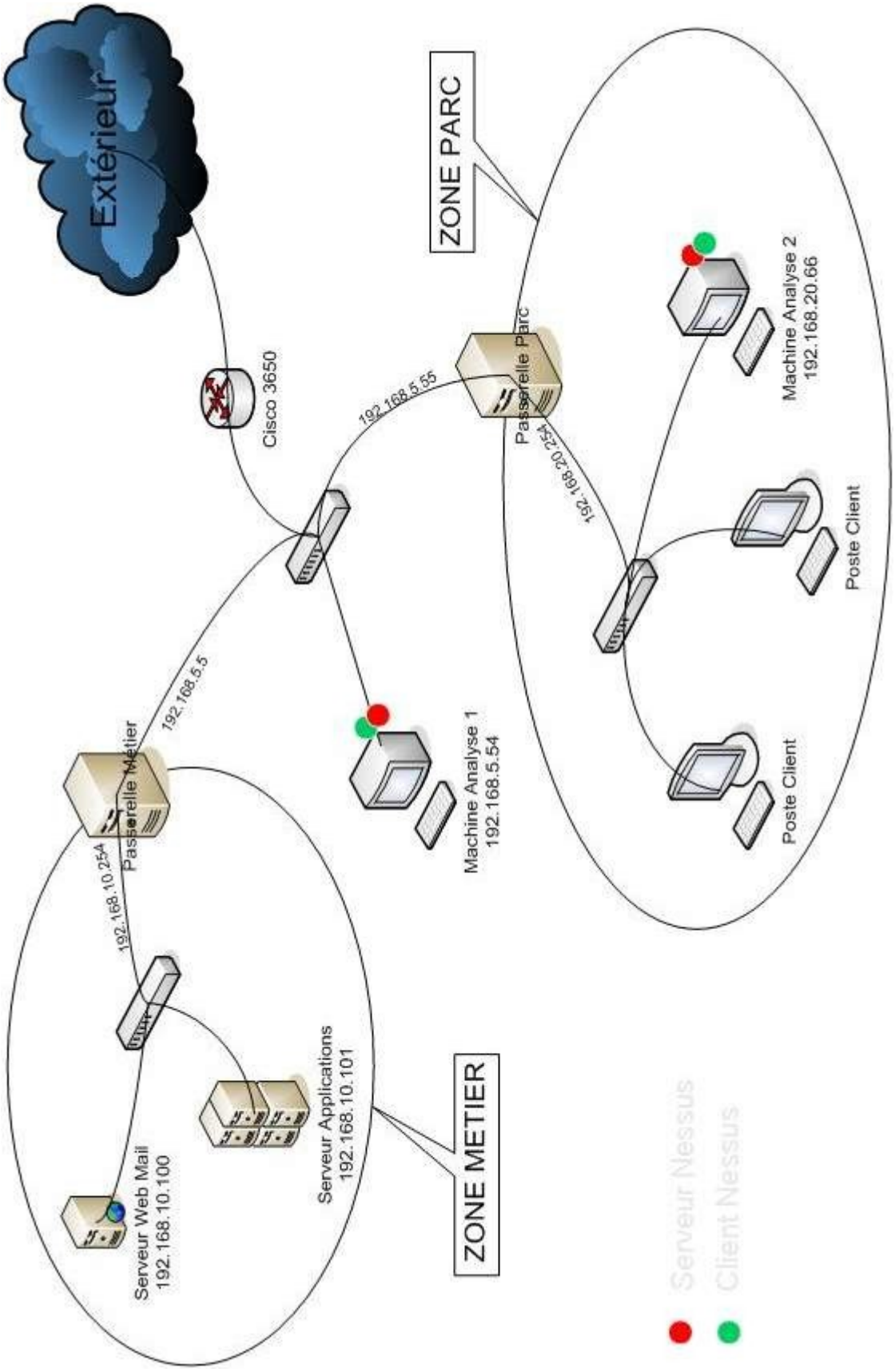
Nessus se compose d'une partie serveur (qui contient une base de données regroupant différents types de vulnérabilités) et une partie client. L'utilisateur se connecte sur le serveur grâce au client et après authentification, il ordonne au serveur de procéder aux tests d'une ou plusieurs machines. Le client reçoit ensuite les résultats du test.

A noter que Nessus est disponible sous Linux et Windows, et est entièrement gratuit.

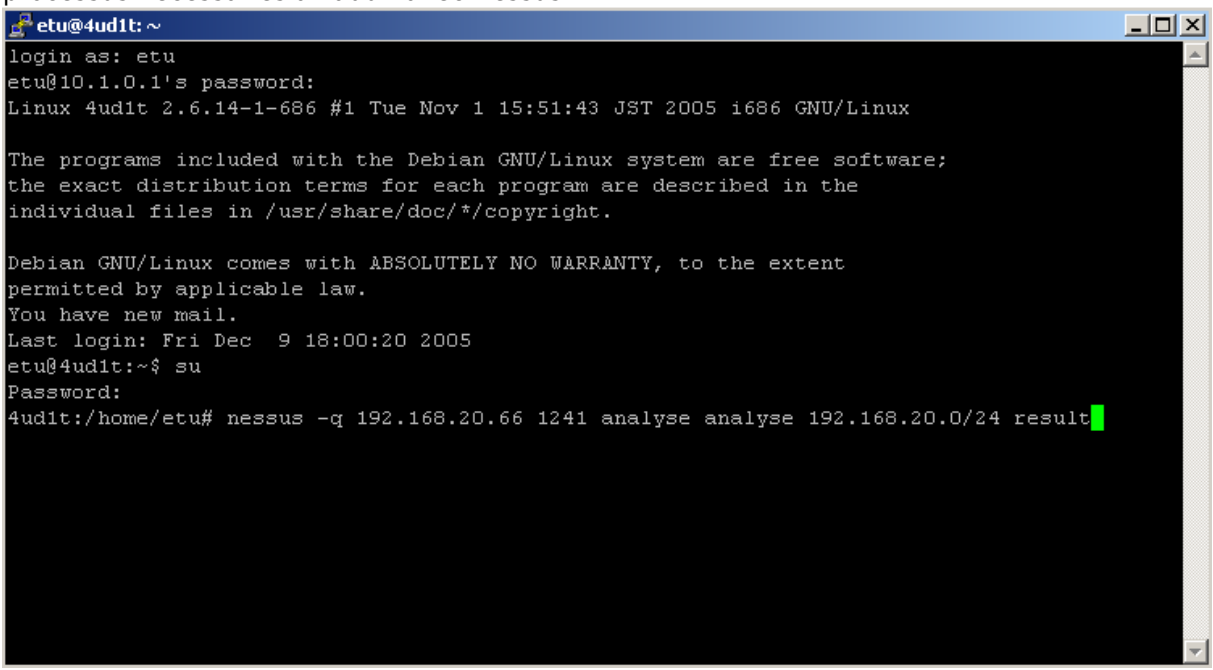
Dans notre cas nous avons répartis les tests de Nessus sur l'architecture de telle manière à réaliser deux tests différents :

- le premier est une analyse interne du réseau : nous avons installé un serveur Nessus sur le poste à l'intérieur du réseau, et un client à l'extérieur du réseau
- le second est une analyse « externe » du réseau : ici nous avons installé le serveur sur le poste mis à l'extérieur du réseau, et le client à l'intérieur du réseau

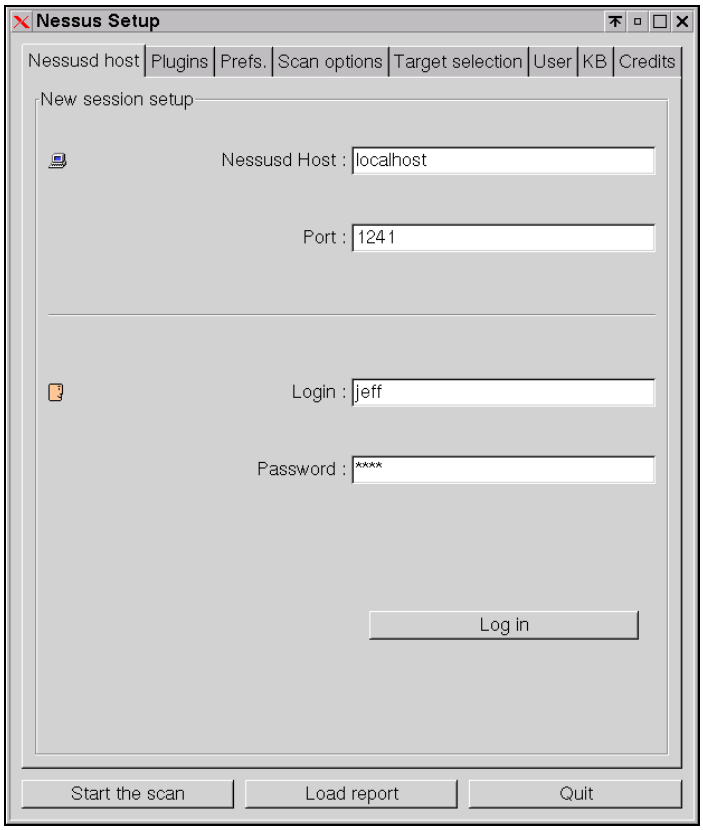
Voici le schéma récapitulatif des essais que nous aurions désiré faire :


Extérieur
ZONE PARC
Cisco 3650
192.168.5.55
Passerelle Parc
192.168.20.254
Machine Analyse 2
192.168.20.66
Poste Client
Poste Client
192.168.5.5
Passerelle Métier
Machine Analyse 1
192.168.5.54
192.168.10.254
Serveur Applications
192.168.10.101
Serveur Web Mail
192.168.10.100
ZONE METIER
Serveur Nessus
Client Nessus

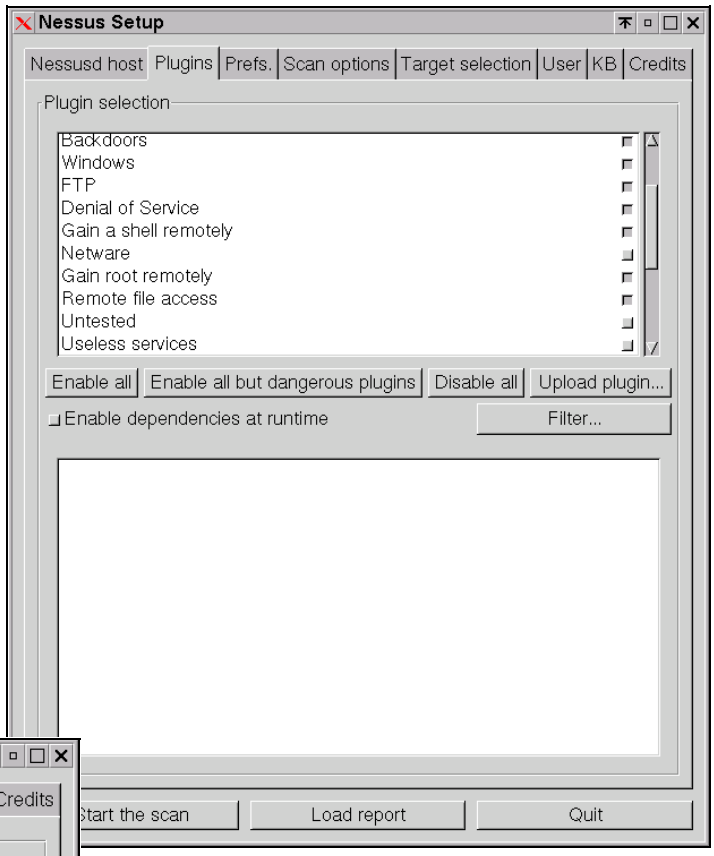
En nous loguant avec OpenVPN (cf partie connexion) et Putty, nous avons pu lancer à distance les processus nécessaires à l'audit avec Nessus :

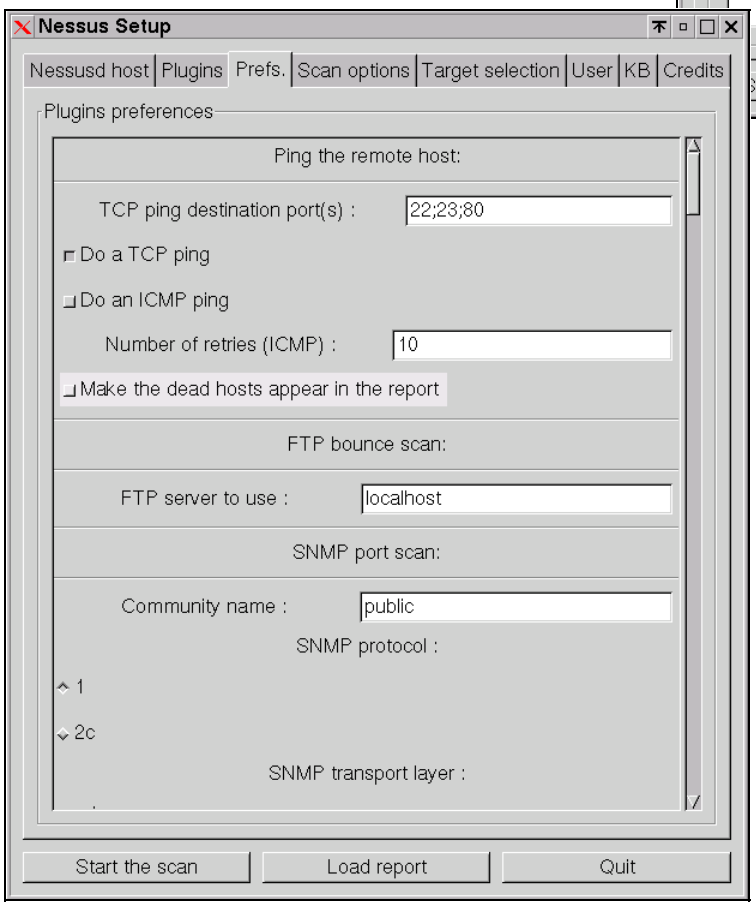


Il faut noter que Nessus possède également une partie cliente en interface graphique, mais nous nous sommes centrés sur le mode *console* puisque les machines que nous avions préparées ne disposaient pas d'interface graphique.
Nous aurions pu aussi lancer Nessus client depuis nos propres PC, ceci aurait donné les copies écran qui suivent :

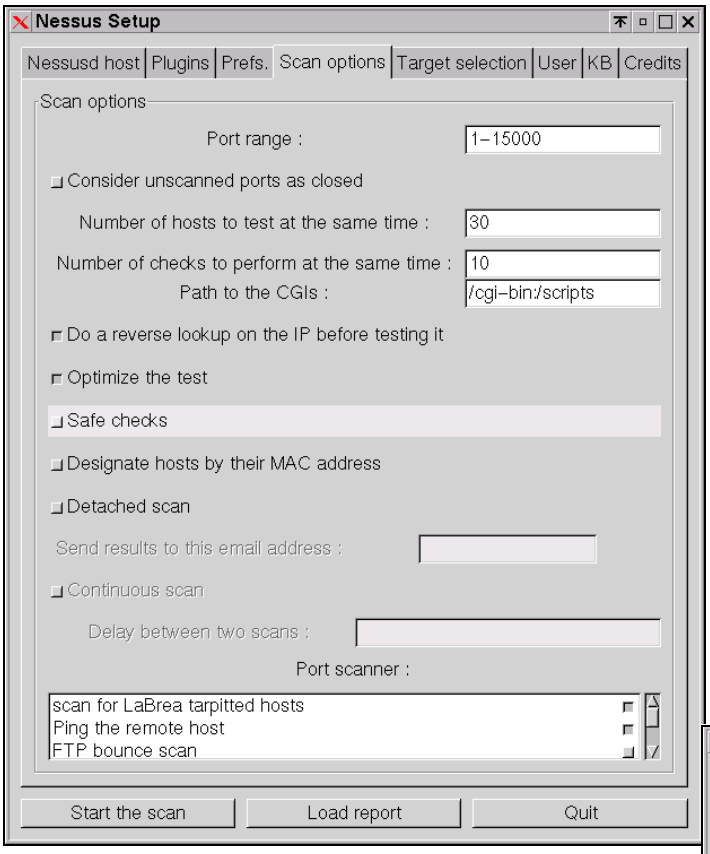


L'outil Nessus permet également d'appliquer et d'utiliser des *Plugins* :





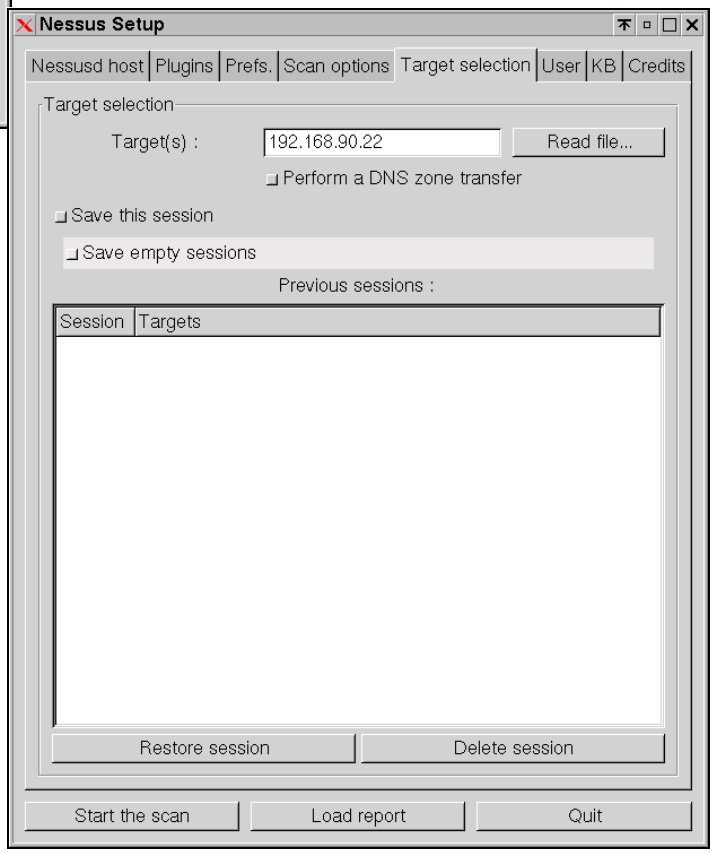
Selon des préférences :



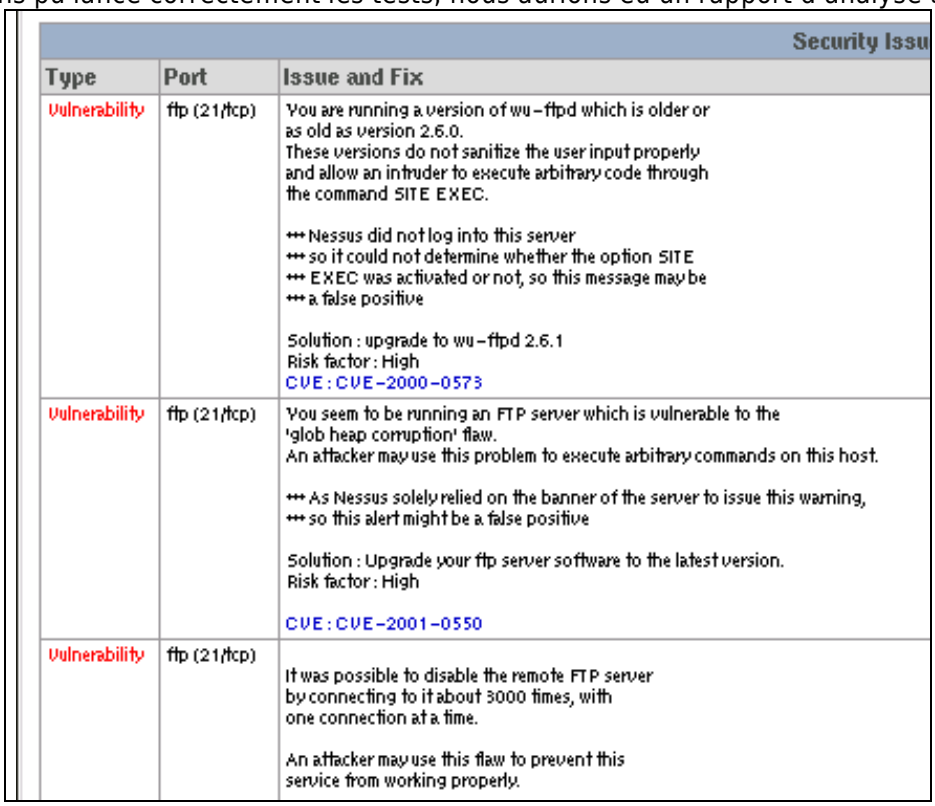
On peut également appliquer des options de scan, tels que :

- la plage de ports testés,
- le nombre d'hôtes testés en même temps,
- etc

Et bien sûr spécifier une cible particulière :



Si nous avions pu lancé correctement les tests, nous aurions eu un rapport d'analyse tel que :



Security Issu		
Type	**Port**	**Issue and Fix**
Vulnerability	ftp (21/tcp)	You are running a version of wu-ftpd which is older or as old as version 2.6.0. These versions do not sanitize the user input properly and allow an intruder to execute arbitrary code through the command SITE EXEC. *** Nessus did not log into this server *** so it could not determine whether the option SITE *** EXEC was activated or not, so this message may be *** a false positive Solution : upgrade to wu-ftpd 2.6.1 Risk factor : High CVE : CVE-2000-0573
Vulnerability	ftp (21/tcp)	You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host. *** As Nessus solely relied on the banner of the server to issue this warning, *** so this alert might be a false positive Solution : Upgrade your ftp server software to the latest version. Risk factor : High CVE : CVE-2001-0550
Vulnerability	ftp (21/tcp)	It was possible to disable the remote FTP server by connecting to it about 3000 times, with one connection at a time. An attacker may use this flaw to prevent this service from working properly.

L'équipe défense et nous-mêmes avons eu de nombreux problèmes à faire marcher la procédure de tests.

En effet la mise à jour des tables iptables a été des plus complexe, l'équipe défense a finalement réussi à les mettre en place (ceci pour la phase 1) et à les rendre actifs pour nos tests.
Malheureusement l'équipe défense ne nous a pas mis en place les iptables nécessaires à la réalisation d'audit sur la phase 2. De plus mettre en place la phase 2 le 10 décembre ne nous a pas aidé à réaliser les audits souhaités. Ceci est regrettable.

Malheureusement un problème « Connexion SSL » nous a empêché de venir à bout des tests de vulnérabilités lancés par le serveur sur le réseau.
Néanmoins, nous avons pu constater « en live » les différentes attaques, celle-ci étant répertoriées sur le par feu administré par l'équipe Défense.

Conclusion

Ce travail d'analyse a été pour nous très constructif. En effet, plusieurs approches ont été vérifiées lors de ce projet qui nous a permis d'avoir un aperçu des difficultés à affronter pour réaliser un bon travail d'audit constructif et efficace.

L'audit de sécurité consiste en une analyse assez vaste du réseau informatique d'une société par une société tiers. Cet audit peut être ciblé sur certains aspects de la sécurité informatique. Il s'étant de la simple vérification des services ouvert sur les terminaux que du social engineering (qui lors de ce projet a été utilisé).

Le travail consiste en plusieurs étapes nécessitant une veille technologique importante ainsi qu'une préparation d'un plan d'action. L'analyse doit être structuré pour ne pas passer à coté de failles importantes. Il est nécessaire également de mettre en place des sondes pour pouvoir vérifier sur des machines neutres les différents types de trafic circulant sur le réseau informatique. Il est également possible d'effectuer des testes d'intrusions permettant d'évaluer le niveau de sécurité des points névralgique de l'infrastructure analysée.

Dans un premier temps, le premier obstacle a été assurément la communication entre notre groupe et celui de la défense. Nous étions là pour les aider, les soutenir dans leurs efforts ainsi que leurs faciliter le travail. Il a été très difficile d'avoir les quelques renseignements dont nous avions besoins pour commencer à travailler. Ceci nous a confronté à une véritable réalité ; les audits se font dans le même état d'esprit.

Nous avons également rencontré des problèmes de communication au sein même de notre groupe. La communication ne fonctionnait pas toujours, certains n'étaient pas consultés et le travail effectué s'en est trouvé d'une incohérence assez importante. Il a été très dur de mener à bien ce projet mais cela a été très constructif. Nous avons tous compris l'importance de l'organisation et l'harmonisation de notre travail. Le but du projet étant de nous mettre en situation réelle, il est normal qu'il n'ait pas été plus encadré sur le plan organisationnel. Nous aurions du certainement nous réunir à plus de reprise et produire des notes, de la documentation et des rapports avec beaucoup plus d'abondance. Ce point a amplement été négligé et a entraîné une désorganisation importante dans notre entreprise. Heureusement, nous apprenons de nos erreurs. Le projet a donc été largement bénéfique à toute l'équipe d'analyse.

Annexe 1 : Engagement de responsabilité

Contrat d'engagement et de confidentialité pour la collaboration des groupes Défense et Analyse

---

Le **groupe Analyse**, s'engage à garder tous les enregistrements, y compris la notation spécifique et détaillée de toutes les frappes et discussions verbales, de toutes les activités pendant l'essai de pénétration et de vulnérabilité.

Ces informations étant suffisamment détaillées pour refaire le test au besoin.

Il assure de garder tous les résultats confidentiels qui restent la propriété de l'organisation.
Tous les résultats des tests de pénétration et de vulnérabilité seront gardés sous le contrôle de l'organisation.

Les membres de l'audit réalisant les tests signerons ce document en s'engageant à ne pas divulguer les informations sur la portée des tests et des résultats.

Le contrat énonce les frontières et la portée du travail à exécuter, la propriété des résultats et les méthodes des tests, aussi bien qu'exigez la confidentialité et la conduite morale/éthique du conseiller.

En outre, le conseiller externe devra s'assurer par une clause dite " hold harmless"pour atténuer des risques à la suite d'une publication d'information négligemment.

A Toulouse le / /

Signatures :

Contrat d'engagement et de confidentialité pour la collaboration des groupes Défense et Analyse

---

Le **groupe Défense**, s'engage à garder tous les enregistrements, y compris la notation spécifique et détaillée de toutes les frappes et discussions verbales, de toutes les activités pendant l'essai de pénétration et de vulnérabilité.

Ces informations étant suffisamment détaillées pour refaire le test au besoin.

Il assure de garder tous les résultats confidentiels qui restent la propriété de l'organisation.
Tous les résultats des tests de pénétration et de vulnérabilité seront gardés sous le contrôle de l'organisation.

Les membres de l'audit réalisant les tests signerons ce document en s'engageant à ne pas divulguer les informations sur la portée des tests et des résultats.

Le contrat énonce les frontières et la portée du travail à exécuter, la propriété des résultats et les méthodes des tests, aussi bien qu'exigez la confidentialité et la conduite morale/éthique du conseiller.

En outre, le conseiller externe devra s'assurer par une clause dite " hold harmless"pour atténuer des risques à la suite d'une publication d'information négligemment.

A Toulouse le / /

Signatures :

TEST D'INTRUSION

Les **tests d'intrusion** (en anglais *penetration tests*, abrégés en *pen tests*) consiste à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle.

On distingue généralement deux méthodes distinctes :

- La méthode dite « **boîte noire** » (en anglais « *black box* ») consistant à essayer d'infiltrer le réseau sans aucune connaissance du système, afin de réaliser un test en situation réelle ;
- La méthode dite « **boîte blanche** » (en anglais « *white box* ») consistant à tenter de s'introduire dans le système en ayant connaissance de l'ensemble du système, afin d'éprouver au maximum la sécurité du réseau.

Ce test d'intrusion, mettra en évidence une faille. C' est un bon moyen de sensibiliser les acteurs d'un projet. A contrario, il ne permet pas de garantir la sécurité du système, dans la mesure où des vulnérabilités peuvent avoir échappé aux testeurs. L' audit de sécurité permet d'obtenir un bien meilleur niveau de confiance dans la sécurité d'un système étant donné qu'ils prend en compte des aspects organisationnels et humains et que la sécurité est analysée de l'intérieur.

PHASE DE DETECTION D'INCIDENTS

Afin d'être complètement fiable, un système d'information sécurisé doit disposer de mesures permettant de détecter les incidents.

Il existe ainsi des systèmes de détection d'intrusion (notés *IDS* pour *Intrusion Detection Systems*) chargés de surveiller le réseau et capables de déclencher une alerte lorsqu'une requête est suspecte ou non conforme à la politique de sécurité.

La disposition de ces sondes et leur paramétrage doivent être soigneusement étudiés car ce type de dispositif est susceptible de générer de nombreuses fausses alertes.

Il est essentiel d'identifier les besoins de sécurité d'une organisation afin de déployer des mesures permettant d'éviter un sinistre tel qu'une intrusion, une panne matérielle ou encore un dégât des eaux. Néanmoins, il est impossible d'écarter totalement tous les risques et toute entreprise doit s'attendre un jour à vivre un sinistre.

Dans ce type de cas de figure la vitesse de réaction est primordiale car une compromission implique une mise en danger de tout le système d'information de l'entreprise. De plus, lorsque la compromission provoque un dysfonctionnement du service, un arrêt de longue durée peut être synonyme de pertes financières. Enfin, dans le cas par exemple d'un défaçage de site web (modification des pages), la réputation de toute l'entreprise est en jeu.

PHASE DE REACTION

La phase de réaction est généralement la phase la plus laissée pour compte dans les projets de sécurité informatique. Elle consiste à anticiper les événements et à prévoir les mesures à prendre en cas de pépin.

En effet, dans le cas d'une intrusion par exemple, il est possible que l'administrateur du système réagisse selon un des scénarios suivants :

- Obtention de l'adresse du pirate et riposte ;
- Extinction de l'alimentation de la machine ;
- Débranchement de la machine du réseau ;
- Réinstallation du système.

Or, chacune de ces actions peut potentiellement être plus nuisible (notamment en termes de coûts) que l'intrusion elle-même. En effet, si le fonctionnement de la machine compromise est vitale pour le fonctionnement du système d'information ou s'il s'agit du site d'une entreprise de vente en ligne, l'indisponibilité du service pendant une longue durée peut être catastrophique.
Par ailleurs, dans ce type de cas, il est essentiel de constituer des preuves, en cas d'enquête judiciaire. Dans le cas contraire, si la machine compromise a servi de rebond pour une autre attaque, la responsabilité de l'entreprise risque d'être engagée.
La mise en place d'un plan de reprise après sinistre permet ainsi d'éviter une aggravation du sinistre et de s'assurer que toutes les mesures visant à établir des éléments de preuve sont correctement appliquées.
Par ailleurs, un plan de sinistre correctement mis au point définit les responsabilités de chacun et évite des ordres et contre-ordres gaspilleurs de temps.

RESTAURATION

La remise en fonction du système compromis doit être finement décrit dans le plan de reprise après sinistre et doit prendre en compte les éléments suivants :

- **Datation de l'intrusion** : la connaissance de la date approximative de la compromission permet d'évaluer les risques d'intrusion sur le reste du réseau et le degré de compromission de la machine ;
- **Confinement de la compromission** : il s'agit de prendre les mesures nécessaires pour que la compromission ne se propage pas ;
- Stratégie de sauvegarde : si l'entreprise possède une stratégie de sauvegarde, il est conseillé de vérifier les modifications apportées aux données du système compromis par rapport aux données réputées fiables. En effet, si les données ont été infectées par un virus ou un cheval de Troie, leur restauration risque de contribuer à la propagation du sinistre ;
- Constitution de preuves : il est nécessaire pour des raisons légales de sauvegarder les fichiers journaux du système corrompu afin de pouvoir les restituer en cas d'enquête judiciaire ;
- Mise en place d'un site de repli : plutôt que de remettre en route le système compromis, il est plus judicieux de prévoir et d'activer en temps voulu un site de repli, permettant d'assurer une continuité de service.

REPETITION DU PLAN SINISTRE

La répétition du plan de sinistre permet de vérifier le bon fonctionnement du plan et permet également à tous les acteurs concernés d'être sensibilisés, au même titre que les exercices d'évacuation sont indispensables dans les plans de secours contre les incendies.