PROJET DE SECURITE : GROUPE ANALYSE

Réalisé par :

Alcaraz Jeremy
Bastien Remi
Chane-To Sébastien
Daunis Nicolas
Gouret Mathieu
Laraki Ilham
Le Louarn Pierre-Yves
Leroux Gillian
Mechhour Youssef
Milano Yannick
Mouron Sébastien
Tinelli Vincent
Vivier Yoann
Valentie Remy

STRI | Télécoms & Réseaux |

Université Paul Sabatier TOULOUSE III

Master 2 STRI — Université Paul Sabatier — 2009/2010

Table des matières

I. Introduction

Les systèmes d'information sont aujourd'hui de plus en plus ouverts sur Internet. Cette ouverture, a priori bénéfique, pose néanmoins un problème majeur : il en découle un nombre croissant d'attaques. La mise en place d'une politique de sécurité autour de ces systèmes est donc primordiale.

Outre la mise en place de pare-feux et de systèmes d'authentification de plus en plus sécurisés, il est nécessaire, pour compléter cette politique de sécurité, d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions.

La plupart des entreprises de moyenne et grande taille déploient, à leur manière, une politique de sécurité. Quelle soit minimaliste ou omniprésente, cette dernière se doit d'être périodiquement auditée, pour plus de performance et d'efficacité.

En application au cours de sécurité des systèmes d'information, dans le cadre du master 2 STRI, le projet que nous devons réaliser consiste à superviser le parc informatique de la PME appelée CANDIDE SA.

Notre projet comportera deux rapports détaillés qui donneront un fidèle aperçu du travail que nous avons fourni au cours de ces derniers mois.
Au cours de ce document, nous verrons les méthodes et les outils utilisés par les sociétés d'Audit afin de surveiller l'infrastructure d'une entreprise. Nous présenterons les constats lors des différentes confrontions ainsi que les résultats de nos outils. Dans le second rapport, nous définirons la politique de sécurité que nous avons suivi plus précisément la norme Ebios. Nous expliquerons ensuite comment se protéger efficacement face à ces intrusions, nous énumèrerons les erreurs commises par la société Candide SA et leurs faiblesses. Enfin, nous établirons les préconisations qu'il faut adopter pour avoir un système d'information sécurisé.

II. Présentation du projet

1. Notre rôle

L'audit, qui regroupe généralement le conseil et l'analyse. C'est un ensemble de services adaptés aux besoins sécuritaires actuels des entreprises. L'audit va analyser les choses sur place en prenant connaissance du système de sécurité de l'intérieur, ce qui permet donc un rapport plus complet sur les améliorations à apporter.

2. Nos objectifs

Notre audit de sécurité va porter sur deux fronts principaux :

- un examen interne des systèmes à la recherche des "grands classiques"
- une recherche par tentative d'intrusion, éventuellement aidé par des logiciels ou des scanners de vulnérabilité.

Voici les objectifs que nous nous sommes fixés :

- Travailler en équipe avec une bonne coordination
- Faire preuve d'une grande communication à l'intérieur de l'équipe mais également avec l'équipe défense
- Comprendre la mise en place de la sécurité informatique
- Trouver les failles de l'infrastructure de la défense
- Analyser et déchiffrer les logs pour en informer le groupe Défense de l'état de son réseau
- Réagir vite suite à un déni de service et en informer le groupe défense
- Simuler des intrusions sur le réseau pour tester les moyens mis en place par le groupe Analyse et le groupe Défense et mettre à l'épreuve l'infrastructure défense
- Conseiller le groupe défense pour améliorer leur sécurité et leurs donner une liste de préconisations

3. Nos contraintes

Tous d'abord nous avons été freinés par le côté obscur de notre tâche d'analyse. Il fallait d'abord comprendre le rôle de l'analyste afin d'adopter la meilleure stratégie.

De plus, Nous avons débuté ce projet avec très peu d'informations concernant les autres équipes, et il nous a donc fallu attendre la première architecture proposée par la Défense pour commencer à établir notre champ d'action. Néanmoins nous en avons profité pour nous documenter sur les différents outils susceptibles de correspondre à notre tâche et de les tester sur nos machines virtuelles afin d'évaluer leurs efficacités. Cependant, nous avons dû faire face à la méfiance du groupe défense à notre égard qui refusait au départ de nous donner des accès à leurs machines pour l'installation de nos outils.

Comme dans la plupart des projets, il y a toujours quelques variations entre ce qui est planifié initialement et ce qui se passe réellement. Ces variations peuvent êtres dues à des modifications des tâches ou bien, dues à des contraintes qui retardent leur l'exécution. En effet, Les attaques n'étant pas virulentes, nous avons dû changer de stratégie vis à vis de notre rôle. Ce qui explique les tests des différents outils d'Audit tout au long de ce rapport et leurs comparaisons.

Toutes ces raisons nous ont donc entravés dans la réalisation d'un échéancier prévisionnel l'avancement du projet. Néanmoins, nous sommes aujourd'hui capable de prévoir l'organisation et la durée du travail avec beaucoup plus de précision, et ceci afin de satisfaire au mieux le client.

4. Organisation de l'équipe

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

- un groupe technique qui se chargera de l'installation des outils
- un groupe rédactionnel dont le rôle est de rédiger les rapports d'audits, les comptes rendu de réunion …
- un groupe communication qui se charge du dialogue et des négociations avec le groupe défense.

Cette répartition n'a pas fonctionné car tout nous nous sommes rendu qu'il était plus facile que l'équipe technique qui réalise une tâche, rédige et explique ses outils. De plus la chargé de travail était inégalement répartie. Ainsi, la nouvelle répartition que nous avons choisie nous a permis de travailler plus efficacement.

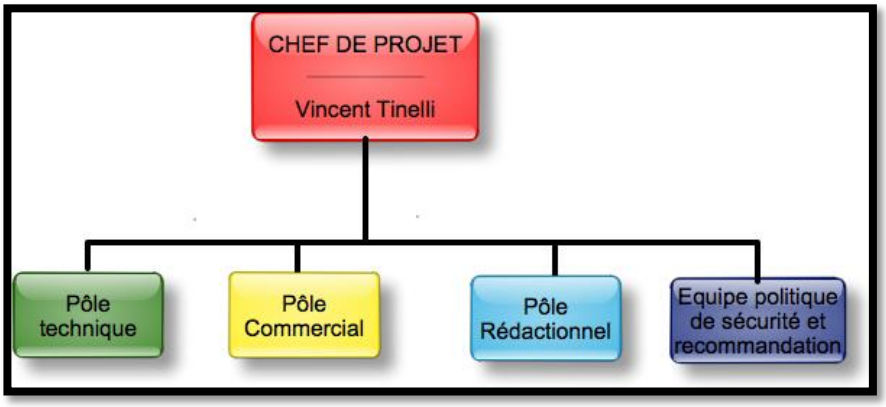
Voici la nouvelle répartition :

- un groupe qui teste les outils
- un groupe de chargeant de l'installation des outils et de l'audit active c'est à dire des outils permettant de réaliser des tests d'intrusions
- un groupe communication
- un groupe qui définie la politique de sécurité, qui analyse les faiblesses de la défense selon nos résultats et se charges des préconisations

Chaque regroupe rédige ses tâches.

De plus, 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.
Résultat, aucune structure, tout le monde partait dans tous les sens sans aucune écoute. Nous avons imposé une hiérarchie référent car il était Très difficile pour la personne qui coordonnait l'équipe.

5. Partage des tâches



Activités	Personnels	Objectifs
Communication	Gouret Mathieu Leroux Gillian Vivier Yoann	Relation Client Etablissement du contrat d'audit
Aspects Techniques	Alcaraz Jérémy Bastien Rémi Chane-To Sebastien Daunis Nicolas Gouret Mathieu Laraki Ilham Le louarn Pierre Yves Leroux Gillian Mechhour Youssef Mouron Sebastien Tinelli Vincent Valenti Rémi Vivier Yoann	Choix des logiciels et outils Choix de l'architecture Déploiement, analyse et veille Rédaction
Administratif	Daunis Nicolas Laraki Ilham	Mise en forme des documents Rédaction des rapports
Gestion de projet & Organisation de l'équipe	Tinelli Vincent Gouret Mathieu Laraki Ilham	Gestion du temps Bilan
Préconisations & Norme Ebios	Daunis Nicolas Laraki Ilham Milano Yannick Tinelli Vincent	Etablissement d'une liste de préconisation pour Candide SA

Le pôle activités communication est chargé de gérer toutes les communications avec l'équipe « défense » : négociation des contrats, planification des sessions d'attaque. Une trace de chaque communication sera conservée.

Le pôle technique est quant à lui seul en charge du cœur de notre métier : l'audit. Ce pôle se charge de proposer et déployer une architecture d'audit appropriée. Il se charge aussi de choisir et de mettre en œuvre les outils d'analyse pertinents.

Le pôle administratif se charge du rassemblement des documents et de la rédaction des différents documents.

Le pôle suivi de projet est en charge de la planification et de la gestion du temps. Dans un premier temps, il établira un planning prévisionnel qui sera tenu à jour tout au long de la durée du projet. Le chef de projet se chargera également du management des différents pôles : suivi des tâches, bilan sur les actions, réorganisation du travail…

Le pôle Préconisations est en charge de l'étude concernant les recommandations à apporter à la société CANDIDE SA

6. Grille des tâches détaillées

	Tineli	Vivier	Gouret	Mouron	Chane-To	Laraki	Daunis	Alcaraz	Leroux	Bastien	Valenti	Mechhour	Lelouarn	Milano
Taches d'installation														
Installation des machines	X	X	X	X										
Installation des outils de supervision et détection	X		X	X										
Installation Nagios		X			X									
Installation et puces des claviers pour l'audit active	X			X						x				
Partie technique														
Rédaction sur Confiker			X											
Rédaction sur Nagios		X			X									
Test et Rédaction sur l'outil Cacti						X	X							
Rédaction sur l'outil MBSA						X	X							
Rédaction Définition Monitoring/Supervision							X							
Rédaction Acid, Snort et Netflow	X		X											
Rédaction attaques avec keylogger	X			X										
Etude Audit WEB 2.0											X	X	X	
Etude alienvolt								X	X					
Etude Backtrack et Avantage live cd				X						X				
Rédaction Metasploit et Nessus											X	X	X	
Etude Zabix & comparaison avec d'autres outils					X			X						
Partie administratif														
Rassemblement des documents, finalisations, cohérence et mise en forme des différents rapports						X	X							
Gestion de projet, du temps et de l'équipe	X		X			X								

	Tineli	Vivier	Gouret	Mouron	Chane-To	Laraki	Daunis	Alcaraz	Leroux	Bastien	Valenti	Mechhour	Lelouarn	Milano
Rapports destinés à la défense														
Rédaction Sur la partie Communication		X	X						X					
Compte rendu des Confrontations	X	X	X						X	X				
Compte Rendu des Pertes de Données	X													
Charte d'utilisation des postes de travails											X	X	X	
Autres: Rédaction du second rapport														
Rapport sur les préconisations, les faiblesses et bilan de l'existant						X	X							
Rédaction de la norme EBIOS														X
Analyse des risques														X

III. Communication Défense/Analyse

1. Le rôle de l'analyste :

Le rôle d'analyste est un métier qui demande de multiples compétences que ce soit :

- Compétences en communication
- Compétences techniques
- Compétences relationnelles

Les compétences en communication interviennent le plus souvent lors de l'établissement du contrat. Il est nécessaire de pouvoir faire passer des informations aux responsables de la société de manière limpide et claire même si celles-ci peuvent être contraire à leur habitude mais indispensable à notre analyse.
Les compétences techniques sont utilisés ici pour l'installation des outils de supervision tels que les sondes, les outils de supervision, pouvoir analyser le réseau en place, proposer des améliorations physique mais aussi l'analyse des logs afin de détecter les éventuelles intrusions ou virus.
La troisième compétence est un peu particulière car elle s'acquiert au fur et a mesure des expériences et est indispensable car elle permet de garder un bon contact entre les intervenants de l'entreprise et ainsi pouvoir proposer des suggestions fondées et pouvant apporter des améliorations notable au sein de l'entreprise. Mais généralement ses nouvelles préconisations sont difficilement acceptées par l'entreprise d'où intervient la compétence relationnelle aidant grandement à faire passer ces idées et/ou demander des accès un peu plus larges et moins restreints.
Voici les différents points que nous avons pu mettre en avant tous au long de cette période avec la société Candide S.A.
Nous commencerons tous d'abord dans cette partie par vous montrer les différents processus de communication.

2. Les processus de communication

La première étape constituait à la création du contrat nous liant avec la société Candide S.A.
Pour cela nous avons dans un premier temps :

- Crée un questionnaire (disponible en annexe)
- Nous avons par la suite proposé une date pour un rendez vous afin de répondre au questionnaire.
- Suite à ce questionnaire, nous avons signé le contrat après deux modifications de leur part.

- Puis à la signature du contrat nous avons reçu de leur part un canal d'échange spécifique, puis l'architecture.

Le contrat avait pour objectifs principaux:

- Connaître l'organisation de l'équipe défense, ainsi que le rôle de chacun au sein de cette équipe afin de faciliter la communication.
- Nous spécifier les droits d'accès sur le réseau de la défense.
- Définir l'architecture du réseau de la défense pour la première confrontation, ainsi qu'un aperçu des évolutions envisagées pour la deuxième confrontation.
- Enfin, communiquer le calendrier des confrontations élaborées entre les différentes parties.

Au cours de la période d'analyse nous avons rajouté un avenant mettant en avant la disponibilité du parc.
Nous avons eu deux autres réunions afin de valider la topologie et de régler certains paramètres tels que les sondes et « Nagios ».
Le questionnaire, le contrat et la page de présentation utilisé pour la réalisation de rapport sont disponibles en annexes.
Après avoir vu la partie communications nous allons maintenant nous intéresser aux outils de communication et de sécurisation mis en place en interne et par l'entreprise Candide SA.

3. Outils de communication et sécurisation des outils

Dans cette partie, nous allons présenter les différents outils de communication et de sécurisation que nous avons utilisés pour dialoguer avec la société Candide S.A.
En premier lieu, il nous a fallu choisir l'adresse de messagerie pour communiquer avec le groupe « Défense ». Deux choix s'offraient à nous, soit utiliser l'adresse de messagerie « stri-online » soit utiliser une messagerie commune à tous les membres de la société d'audit. Etant donné que nous n'étions pas complètement sur (possibilité de phishing) de l'adresse de messagerie disponible pour notre formation, nous avons opté pour une adresse commune et externe à la formation : « Gmail ».
Ensuite nous nous sommes intéressés à l'aspect sécurité de l'échange de messages, dans le but de protéger les informations échangées avec la société Candide S .A. Pour cela, le chiffrement et le cryptage des mails étaient indispensables. Le module « FireGPG » a été notre solution, c'est une extension Firefox sous licence MPL qui fournit une interface pour appliquer des opérations GnuPG au texte de n'importe quelle page : chiffrement, déchiffrement, signature et vérification de signature. Ce qui a motivé notre choix pour ce module plutôt qu'un autre, c'est qu'il ajoute des fonctionnalités à l'interface de Gmail (permet d'utiliser GPG directement dans Gmail) et que certains membres de notre équipe l'avaient déjà testé, et qu'ils étaient satisfaits des résultats obtenus.

Chaque individu de l'audit a généré une clé publique qu'il a ensuite envoyée à tous les membres de notre société ce qui nous a permis d'échanger des mails en interne de

manière sécurisé. Puis pour communiquer avec Candide S.A., il a été décidé qu'une seule personne devait faire le lien avec la « Défense », ceci permettant une meilleure organisation pour l'échanges de données en centralisant celle-ci sur une seule et même personne « Mathieu », et ainsi réduire au maximum les pertes d'informations au cas où l'un d'entre nous avait été hacké. Cette communication s'est faite via le webmail sécurisé fournit par la société Candide S.A. dans lequel « Mathieu » devait rentrer un couple « login-mot de passe » ainsi qu'un « SubKey » pour pouvoir s'authentifier et échanger des mails sécurisé avec la société.
Enfin nous avons fait quelques recommandations (ou préconisations), évidente mais qu'il est essentiel de rappeler pour éviter toutes pertes de données, à notre groupe tel que :

- Ne pas envoyer de mail via les PC de la faculté,
- Utiliser de préférence Firefox plutôt que Internet Explorer,
- Ne pas laisser son PC sans surveillance dans les locaux de l'université,
- Ne pas discuter du projet durant les heures de cours et effectuer les réunions dans des salles que nous n'utilisons pas pour notre formation STRI.

Tous ceci évitant, que des personnes mal intentionnées nous volent nos données sensibles et nos mots de passe car ceci aurait entrainé un véritable problème pour nous au vu du contrat que nous avions passé avec la « Défense ».

4. Problèmes rencontrés

Le dialogue et la prise de rendez vous a été assez difficile avec l'équipe communication de la défense. En effet lors de la première réunion, l'équipe communication de la défense ne voulait pas du tout nous laisser d'accès au parc, même restreint.

Lors de la réédition du contrat, la défense a bien voulu nous laisser installer certain plugin et logiciel « sous surveillance » mais pas de création de compte restreint. Suite à une simulation d'attaque de notre part et la diffusion de tous les mots de passes et backups de toutes les machines du parc de la défense, l'équipe défense était assez distante et n'a pas voulu rééditer de contrat avec nous.

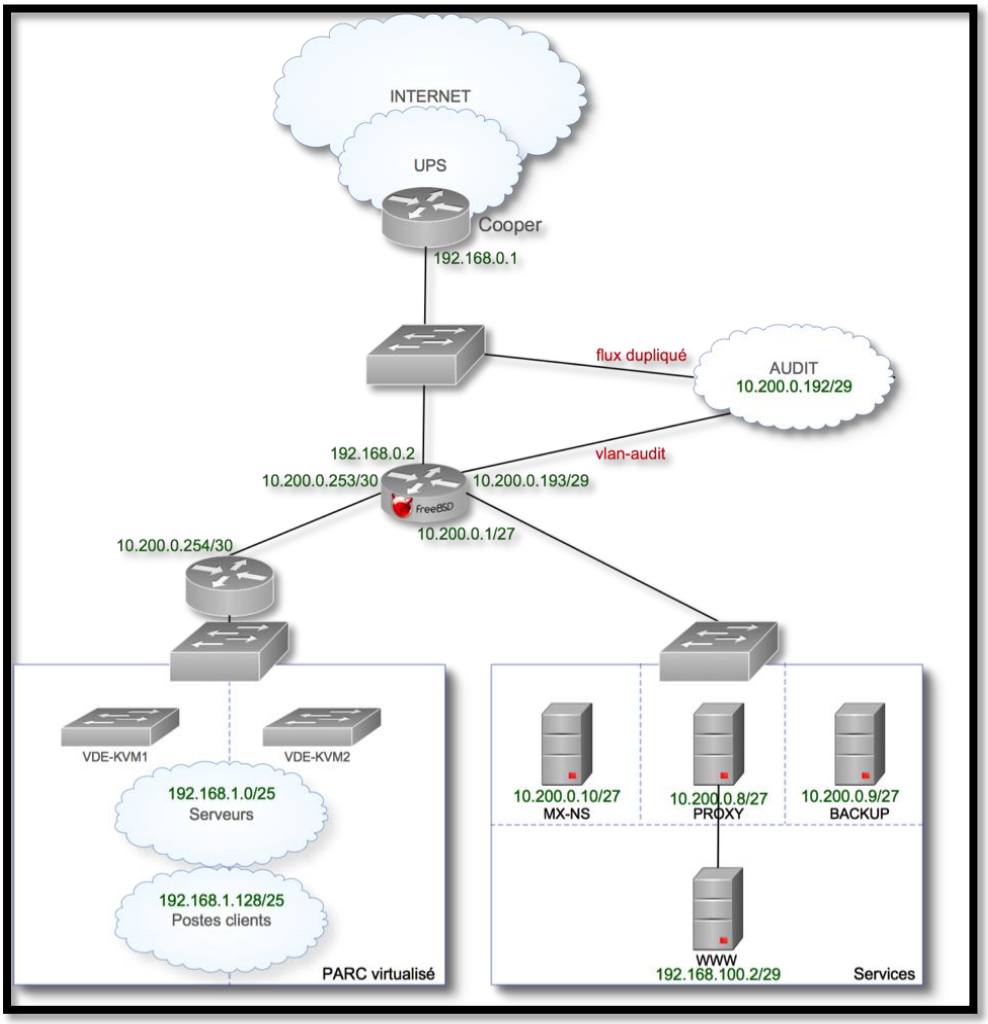
A noter aussi que le délai en début de projet afin de nous attribuer des adresses IP/ports pour l'installation des sondes a été assez long. L'équipe défense ne nous faisait pas part des changements qu'il faisait sur leur architecture lorsqu'il y en avait. Malgré plusieurs demandes depuis le début du projet, l'équipe de la défense ne nous a pas donné sa chartre d'utilisateur

IV. Nos outils utilisés

1. Infrastructure de la défense avec la mise en place de nos outils

Suite à l'établissement de notre contrat avec la société Candide SA, cette dernière nous a dédié un lien dans leur architecture afin d'implémenter nos sondes.

Voici un schéma récapitulatif de l'architecture mise en place :



2. Outils de détection

a. Qu'est ce que la détection ?

La sécurité contre les attaques distantes se renforce, notamment par le biais d'équipements réseaux plus puissants (comme des firewalls plus intelligents), mais les attaques locales restent toutefois encore efficaces : l'ARP Spoofing, le vol de session, … restent souvent possibles.

L'informatique évolue, les applications sont de plus en plus complexes et les délais laissés aux programmeurs et administrateurs sont souvent très (trop) courts. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues.

Les attaques distribuées seront toujours redoutables si la plupart des machines personnelles ne sont pas protégées. Ce qui nous amène à notre nouvelle partie : comment détecter et empêcher ces attaques ?

Détection d'attaques : les IDS

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelé IDS (Intrusion Detection Systems), les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche.

On définit que les IDS sont des ensembles de composants logiciels et matériels dont la fonction principale est de **détecter et analyser toute tentative d'effraction** (volontaire ou non). Et leur fonction première est la détection par des **techniques de sondage** (balayages de ports, fingerprinting), **des tentatives de compromission de systèmes**, **d'activités suspectes internes**, **des activités virales** ou encore **audit des fichiers de journaux** (logs).
Normalement c'est un système capable de détecter tout type d'attaque.

b. L'outils Snort

Snort provient du monde Open Source. Avec plus de 2 millions de téléchargements, il s'est imposé comme le système de détection d'intrusions le plus utilisé. Sa version commerciale, plus complète en fonctions de monitoring, lui a donné bonne réputation auprès des entreprises.
Il est capable d'effectuer une analyse du trafic réseau en temps réel et est doté de différentes technologies de détection d'intrusions telles que l'analyse protocolaire.

De plus il peut détecter de nombreux types d'attaques : *buffer overflows, scans de ports furtifs, attaques CGI, sondes SMB, tentatives de fingerprinting de système d'exploitation* ...

Snort est doté d'un langage de règles permettant de décrire le trafic qui doit être accepté ou collecté. De plus, son moteur de détection utilise une architecture modulaire de plugins

Notons que Snort dispose de trois modes de fonctionnement :

- sniffer de paquets
- logger de paquets
- système de détection/prévention d'intrusions.(Seul mode que nous utilisons ce mode.)

Par défaut, **les alertes de Snort sont enregistrées dans un simple fichier texte**. L'analyse de ce fichier n'est pas aisée, même en utilisant des outils de filtre et de tri. C'est pour cette raison que nous avons décidé de mettre en place un outil de monitoring dénommé Base. Cet outil sera traité dans une partie sous-jacente.

c. L'outil NESSUS

Scanner un réseau avec Nessus

Nessus est un outil d'audit automatique de réseau. . Il signale les faiblesses potentielles ou avérées sur les machines testées. Il permet, via un mode client-serveur, de lancer des attaques sur un réseau ou plusieurs réseaux (partager la charge d'attaque sur ces réseaux avec un client et plusieurs serveurs), donc sur les serveurs que comporte(nt) ce(s) réseau(x). Cet outil possède une base d'attaques importante, et permet ainsi de tester certaines versions obsolètes de services connus (Apache / IIS). Il permet aussi de tester les applications Web connues (très fortement utilisées par la communauté, style PHPNuke, phpBB, et autres). Nessus possède aussi d'autres plugins intéressants comme Hydra, qui permet de tester la robustesse des mots de passe des applications Web.

Nessus est constitué de 2 parties:

- Le serveur qui effectue les tests de sécurité.
- Le client peut être situé sur une autre machine, et invoquer des fonctions distantes sur le serveur afin de tester la sécurité sur une ou plusieurs machines ou réseaux.

Installation

Pour l'installation et la mise en route, des pages très utiles sont:

http://www.nessus.org/demo/first.html

Elles décrivent les étapes d'initialisation du serveur, comme du client nessus et l'utilisation du client. De plus, lorsqu'ils sont bien installés les pages de manuel (man) sont également très utiles, notamment pour le nessus-adduser qui permet de créer de nouveaux utilisateurs. Pour créer un utilisateur la page suivante donne les démarches principales:

http://www.nessus.org/demo/first.html

Configuration

Il faut ajouter des utilisateurs au serveur Nessus pour les autoriser à effectuer des tests de sécurité.

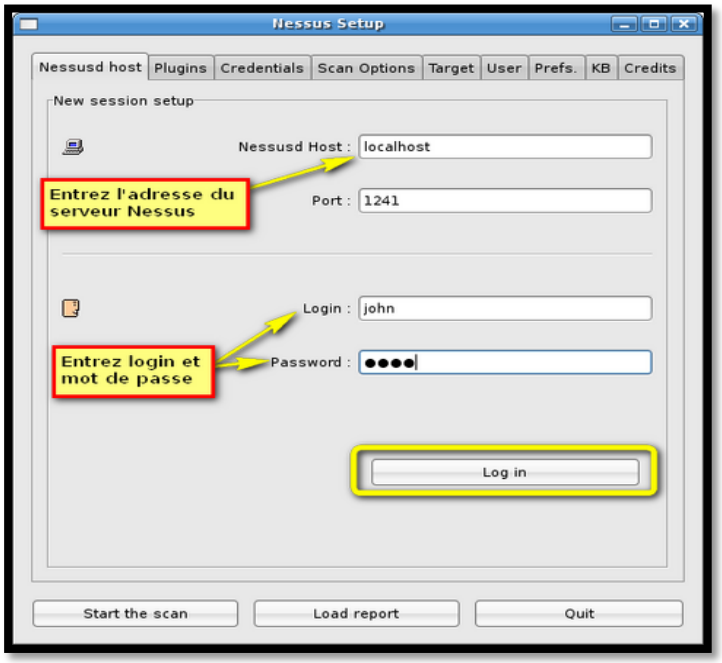
Chaque utilisateur est définit par un login et un mot de passe pour l'authentification ainsi qu'une liste de rôles déterminant ces droits à lancer tel ou tel test mais aussi les réseaux (ou machines) sur les quelles ces tests peuvent être effectuer.

Un mode d'authentification sécurisé peut être mis en place grâce à un certificat que le serveur génère pour les clients potentiels.

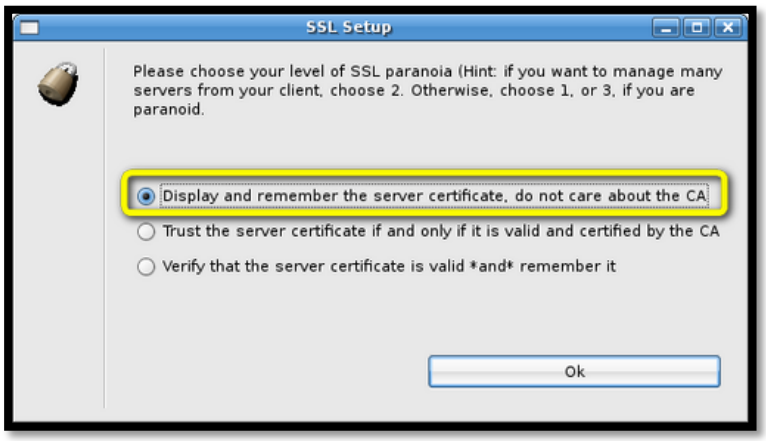
Connexion au serveur NESSUS

Lancez le client Nessus

Entrez l'adresse du serveur Nessus, ainsi que le login et mot de passe, puis cliquez sur le bouton "Log in".



Comme le certificat de votre serveur Nessus n'a pas été signé par une autorité de certification, sélectionnez la première option:



Le certificat sera ensuite affiché: Acceptez-le en cliquant sur Yes.

Utilisation du client NESSUS

Comment se déroule un scan?

Un scan d'une machine se déroule en deux temps. Tout d'abord il scanne des ports d'après les critères définis dans les préférences, puis soumet les machines scannées à des attaques pour voir les machines sensibles à des attaques. Ces attaques sont sélectionnées par les plugins dans la rubrique du même nom.

Par défaut, les plugins risquant de planter les machines à tester son désactivés. (Nessus nous avertis d'ailleurs de cela par une petite fenêtre pop-up.)

Les différentes rubriques et onglets

Nous allons passer en revue les principaux onglets qui sont les suivants:

- **L'onglet Plugin** nous permet de choisir quels tests effectuer.
- **L'onglet Credentials** nous permet de fournir éventuellement des logins/passwords pour accéder aux machines à tester.
- **Scan options** nous permet de choisir quels ports tester et la manière de détecter un port ouvert.
- **Target** permet de choisir quoi tester: Vous pouvez entrer l'adresse IP, le nom de la machine ou encore l'adresse IP du réseau à tester.
- **L'onglet préférence** permet de choisir les techniques employées lors du scan de ports.

Nous allons détailler l'onglet Plugins

- Cet onglet concerne les plugins de nessus. Ils sont sollicités dans la seconde phase du scan des machines. Ils contiennent des attaques réseau connues et servent pour tester la vulnérabilité des machines aux attaques sélectionnées.
- Une fenêtre présente les différents plugins disponibles alors qu'une autre affiche les différentes attaques décrites par le plugin sélectionné. Des boutons radio permettent de sélectionner les plugins à mettre en œuvre et chaque attaque à tester.
- Il y'a possibilité de charger des plugins supplémentaires pour mettre à jour la base des attaques testées par nessus.
- Un point important est que nessus signale toute attaque pouvant faire crasher la machine visée lors de la sélection d'une attaque.

Principaux paramètres

Recherche de port SNMP:

La version SNMP, la communauté, le protocole de couche transport sont paramétrables, ainsi que la plage de ports et la répartition temporelle.

Ping de l'hôte distant:

Choix entre ICMP Ping ou TCP Ping et traitement des hôtes absents et du log des hôtes découverts.

Fonctionnalités de nmap:

Ceci comprend :

- Les techniques de scan TCP (connect(), SYN, FIN, Xmas tree, null scan et les composés de plusieurs techniques).
- Les différentes options de nmap telles que le scan de ports UDP, de ports RPC, la détection d' OS, la fragmentation de paquets IP, le scan aléatoire...
- La répartition temporelle est paramétrable, que ce soit dans la fréquence aussi bien que dans la régularité.

IDS:

Des techniques de camouflage d'intrusions sont sélectionnables à travers une dizaine de techniques proposées. Elles permettent de flouer un éventuel IDS qui serait en train d'observer le réseau.
Chacune tire parti de failles différentes connues de certains IDS du commerce.

NIDS:

De nombreuses techniques d'évasions spécifiques à certains protocoles tels TCP ou HTTP sont proposées ici pour flouer les détecteurs d'intrusions.

Brute Force:

Possibilité de tester en Brute Force (essai de toutes les possibilités) sur de nombreux protocoles: Telnet, pop3, IMAP, VNC, FTP...

Autres:

D'autres paramètres sont également configurables, mais concernent des techniques avancées spécifiques et ne seront donc pas développées ici.

Scan options:

Les options de scan sont d'ordre général :

a. Par exemple les plages de ports à scanner, le nombre d'ôtes à scanner à la fois... et d'autres options tout aussi générales.
b. Egalement une possibilité de faire exécuter le scan en tache de fond.

Target sélection:

Permet de sélectionner les machines cibles par adresses IP ou réseaux ou sous réseaux.

Avantage :

a. Nessus est un outil très complet dans son domaine. Les paramètres sur lesquels on peut agir sont très nombreux, ce qui donne l'impression que cet outil est très complet.
b. La présentation du rapport de scan est très pratique, sous forme tableau dynamique rassemblant les sous réseaux observés, les IP précises observées, les ports détectés, la sensibilité du port, et enfin une explication sur le warning présenté.
c. L'interface graphique est la bienvenue et peut présenter de manière visuelle toutes les options disponibles.
d. Nessus prévient si l'on coche une option qui peut être dangereuse ou bloquante pour un certain temps.
e. Son architecture permet son extensibilité. Le développement d'une attaque n'est pas très compliqué en langage Nessus (NASL - Nessus Attack Scripting Language), ou même en C.
f. Les informations sur le niveau de sécurité résultant de ces attaques sont reportées dans les rapports. Des explications sont données sur la raison pour laquelle un trou de sécurité a été détecté.

Inconvénients :

1. Le grand nombre de paramètres sur lesquels on peut agir sans tout le temps bien comprendre ce qu'ils font. En effet le détail et la signification des attaques, des options de scans ne sont pas toujours très clairs par leur simple nom.

2. La fermeture du code source depuis la version 3. Les versions antérieures étaient totalement ouvertes sous licence GPL. Nessus est un bon logiciel pour débuter dans la sécurité des réseaux et pour comprendre quels sont les points vulnérables d'un réseau. Il ne remplacera pas cependant une bonne analyse méthodique d'un expert sécurité.

Gestion de priorité

Nessus possède une gestion des droits pour décrire précisément ce qu'a le droit de faire un utilisateur. Par exemple, on peut configurer Nessus pour autoriser un utilisateur à scanner uniquement sa propre machine.

Mises à jour

Il est important de tenir la liste des plugins à jour afin que Nessus soit capable de détecter les dernières failles.

Il faut lancer régulièrement nessus-update-plugins: **sudo nessus-update-plugins**

Précautions

Il est important de tenir la liste des plugins à jour afin que Nessus soit capable de détecter les dernières failles. Il faut lancer régulièrement nessus-update-plugins: **sudo nessus-update-plugins**

3. Outils de monitoring et de supervision

a. Présentation du monitoring et de la supervision

Une entreprise doit posséder un réseau fonctionnel, optimisé, rapide et à la maintenance rapide afin de prévenir tout travers dans le fonctionnement des applications clients/fournisseurs et surtout dans sa production. C'est pourquoi la mise en place de solutions de monitoring/supervision telles que celles que nous avons testées sont des solutions simple, rapide, efficace et bon marché pour une surveillance permanente du réseau.

Qu'est-ce que le monitoring/supervision réseau?

Ces deux termes signifient surveillance, ils permettent donc de connaitre l'activité ou la disponibilité de différents éléments. Cela consiste à suivre l'évolution des différents matériels que compose le réseau de l'entreprise mais aussi du statu des différents serveurs ainsi que de leurs services.

La supervision permet d'indiquer et commander l'état d'un système, de surveiller, visualiser via une interface graphique, mais aussi de faire des comptes rendus des différentes alertes qui remontent et de pouvoir les gérer dans un tableau de port ou via une interface graphique.

L'évolution des différents matériels :

L'évolution des matériels (commutateurs, concentrateurs...) sur un réseau correspond à leur réactivité sur le réseau (temps de latence...) à leur disponibilité sur le réseau (nombre de problèmes de fonctionnement, nombre d'erreur...) ou encore au trafic que ces matériels doivent supporter.

Le statut des différents serveurs :

Le statut d'un serveur correspond ici à sa disponibilité aux clients mais surtout du fonctionnement des rôles qu'il possède : serveur d'impression, de fichiers, proxy... La surveillance de ces paramètres est vitale à la bonne marche du réseau global de l'entreprise.
Ainsi on peut arriver à la différenciation de deux types de surveillance réseau :

La surveillance interne :

Elle sert essentiellement à vérifier les serveurs et les services présents sur l'intranet d'une entreprise. Il s'agit en général d'un logiciel installé sur un ordinateur de l'entreprise (Nagios...)

La surveillance externe :

Elle correspond à une analyse depuis l'extérieur du réseau et simule la visite d'un internaute ; c'est souvent le service d'une entreprise externe qui a déjà ses propres serveurs répartis dans le monde pour analyser le site. Il s'agit donc plus souvent d'un service que d'un outil logiciel, ce qui évite la charge de la mise à jour.

Pourquoi monitorer un réseau?

Il existe plusieurs raisons pour les entreprises de vouloir surveiller son réseau :

- Donne une **vue globale sur le fonctionnement du réseau** de leur entreprise, aussi bien sur la disponibilité des différents serveurs que sur le fonctionnement de services aux personnes chargées du réseau.
- Un réseau surveillé est un gain de temps important dans l'entretien et la **vitesse de réactivité** lorsqu'un problème intervient. Il est possible de connaître un problème avant même que les utilisateurs ne s'en rendent compte. La panne est donc réparer plus rapidement ce qui équivaut en en entreprise à un gain d'argent
- les outils de monitoring peuvent également **aider à la détection** de mauvaises configurations de matériels ou à des conflits de services ou d'IP sur le réseau : grâce à un outil de monitoring réseau il est possible d'avoir une premier bilan du fonctionnement de son réseau.

Les possibilités d'une surveillance réseau :

La surveillance d'un réseau offre, selon les solutions disponibles sur le marché, ce que nous verrons plus tard, des possibilités plus ou moins avancées. Mais de manière générale, toutes les solutions proposent trois grandes catégories de surveillance.

Surveillance des matériels

La surveillance des matériels correspond donc à vérifier divers paramètres sur les matériels réseaux tels que des concentrateurs, commutateurs, ponts, passerelles, proxy, firewall.... Il s'agit d'un rôle critique du fait que ces matériels sont des points de communications primordiaux dans le réseau d'une entreprise, dans la protection de celui-ci et dans sa rapidité.

Comme il a été précisé, chaque matériel offre selon le constructeur plus ou moins de paramètres à surveiller cependant et par convention, les constructeurs ont ouverts les mêmes paramètres par défauts visibles sur leurs matériels.

- Vérifier la présence d'un matériel en testant s'il répond à un Ping.
- Contrôler son temps de réponse au Ping.
- Contrôler son ou ses interfaces réseaux.
- Contrôler le taux d'utilisation de ces composants.
- Contrôler le signal des bornes WIFI, du nombre de clients...

Surveillance des périphériques

Un réseau d'entreprise est composé non seulement de serveurs et de matériels réseau mais également de périphériques réseau tels que des imprimantes, des fax, des photocopieurs....

Ces matériels peuvent également être contrôlés et il est possible de citer :

- Contrôler des taux d'encres
- Contrôler les files d'attente des documents
- Contrôler le nombre de copies,
- Contrôler le nombre d'utilisateurs....

L'utilité de surveiller des périphériques permet de prévenir les saturations d'imprimantes ou encore d'avoir un rapide aperçu des gauges d'encres disponibles dans le but d'éviter aux utilisateurs de devoir signaler un problème sur un périphérique et de devoir effectuer des tests manuels pour l'identifier.

Surveillance des serveurs

Toute grande entreprise possède aujourd'hui différents serveurs possédant différents rôles plus ou moins critiques. La surveillance de ces rôles tient donc une place essentielle dans le bon fonctionnement du réseau de l'entreprise et parfois même de son commerce. Tout d'abord et avant tout, de leur disponibilité sur le réseau et pour les clients : en effet un serveur qui n'est plus disponible sur le réseau peut engendrer d'énormes problèmes dans une entreprise aussi bien au niveau des utilisateurs que des ressources qui ne sont plus atteignables. Ensuite il y a le temps d'accès à ce serveur qui est aussi un paramètre intéressant : en effet même si les clients ont un accès au serveur, il faut que celui-ci soit le plus rapide possible surtout lorsque qu'il s'agit de serveur de fichiers. Enfin il y a les différents rôles d'un serveur qui peuvent être surveillés.

- serveur DHCP
- serveur DNS
- serveur de MAIL
- serveur WEB

Surveillance des services

En fait il s'agit de vérifier qu'un processus tourne bien sur le serveur et que ce service fournit bien les données souhaitées. Il est également possible de vérifier qu'une tâche s'exécute convenablement ou bien encore qu'un fichier soit bien présent à un endroit précis. L'utilité de la surveillance des services est évidente : le réseau d'une entreprise joue toujours un rôle dans son commerce, sa production ou bien ses communications, c'est pourquoi ce réseau comprend des serveurs sur lesquels tournes des services communs ou spécifiques à l'entreprise. La vérification de la bonne exécution de ces services est donc une tâche importante et critique dans certains cas (Base de données, services de mises à jour, automates....).

Les technologies de monitoring.

Un réseau d'entreprise est composé de nombreux périphériques et ordinateurs aux systèmes d'exploitation souvent différents allant de Windows XP au AIX voir même jusqu'à des automates aux systèmes propriétaires. Pour cette raison les différents constructeurs ont décidé de respecter une convention réseau en utilisant tout un protocole spécifique : SNMP.

Le protocole SNMP

« Simple Network Management Protocol » (SNMP), protocole simple de gestion de réseau en Français, est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux, matériels à distance.

Le système de gestion de réseau est basé sur trois éléments principaux : un superviseur, des nœuds (ou nodes) et des agents. Dans la terminologie SNMP, le synonyme manager est plus souvent employé que superviseur. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface, connectant l'équipement managé (nœud) au réseau et permettant de récupérer des informations sur différents objets.

Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données arborescente appelée MIB (« Management Information Base »). SNMP qui permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

Méthode d'implémentation de la solution

L'implémentation d'une solution de surveillance à une compagnie doit être évaluée et étudiée.

Quels sont les besoins ? Les fonds de la compagnie ? Structure du réseau ?

Pour chacune de ces parties ce ne sont pas les besoins de compagnie à laquelle la solution a été installée mais plutôt d'un point de vue généraliste axé sur les points importants.

Les besoins :

Tout d'abord, la première étude à réaliser est celle des besoins de l'entreprise. Chaque compagnie est différente, tous services ou matériels ne sont pas utiles à surveiller, c'est pourquoi il est meilleur de choisir les éléments les plus appropriés et particulièrement ceux qui jouent un rôle critique dans le réseau de l'entreprise.

Les fonds de la compagnie

Toutes les entreprises ont des fonds limités, c'est pourquoi il est nécessaire de choisir une solution dont les coûts seront minime tout en ayant le maximum de fonctionnalités.
Il y a également les futurs coûts qui devraient être pris en compte c'est-à-dire que l'application produira des bénéfices mais également un gain de temps qui comme nous le savons, représente de l'argent pour les entreprises.
Une analyse doit être effectuée en intégrant les éléments selon :
- le coût de la solution
- le coût en temps d'installation
- le coût de l'entretien de la solution
- les bénéfices produits par l'utilisation de la solution
- le temps sauvé dans l'utilisation de la solution

La structure du réseau

Cette étude est elle-même en plusieurs sous-parties :
- liste des divers matériels réseaux

- organisation du réseau : (VLANs, les firewalls, les routeurs ....)

Conclusion :

Le monitoring joue aujourd'hui un rôle essentiel dans les entreprises car les gains multiples tels que le temps, la réactivité ou encore la prévention sont des facteurs importants et primordiaux pour un réseau dense et complet.
Bien entendu, il n'est pas encore possible de tout contrôler ou de tout faire avec des solutions de surveillance réseau, mais les produits existants aujourd'hui commencent à devenir intéressants, surtout sur la gamme des produits libres.

On peut s'attendre que dans un avenir proches ces solutions seront indispensables à toute entreprise désireuse d'un réseau fiable et efficace qui pourra compter sur la mise en place de solutions peu coûteuses, à la maintenance rapide et fiable et aux services professionnels disponibles.

b. Les outils Nagios et Centreon

Pourquoi Nagios ?

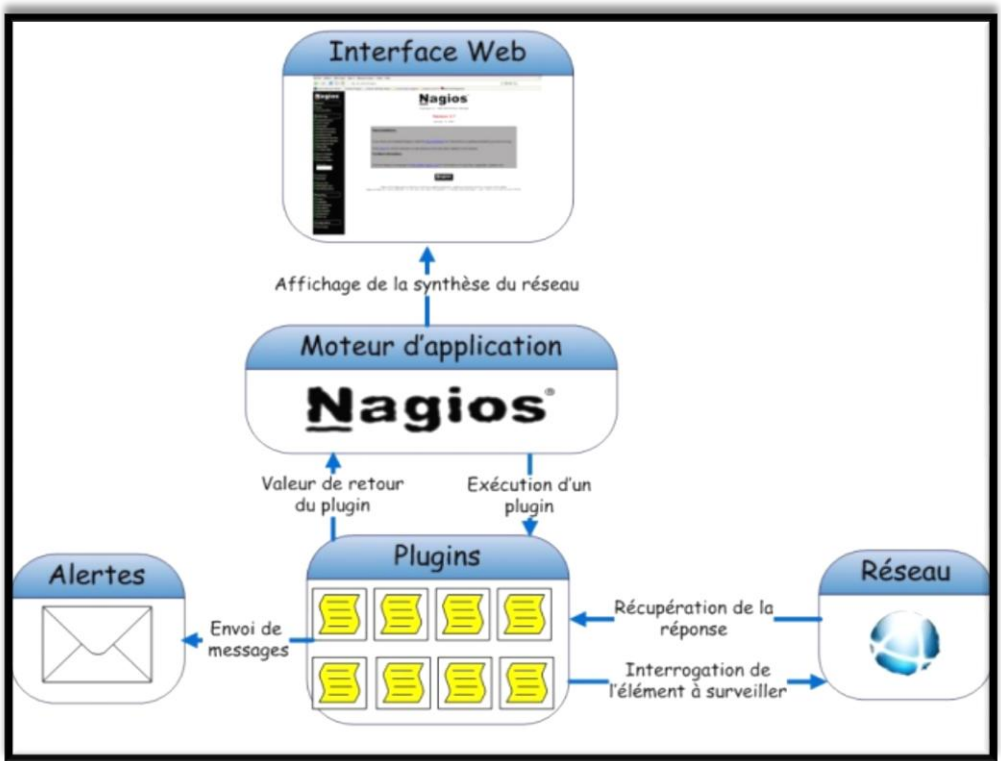
Il faut savoir qu'il existe **une multitude de logiciel libre** afin de faire de la supervision tel que Nagios, Cacti ou encore Zabbix.

Nous avons choisi d'installer la **FAN (fully Automated Nagios)** qui est en faite une compilation de plusieurs logiciels, basée sur une CentOS.

L'avantage de cette distribution est d'être une solution facile d'installation et de réinstallation. C'est également une solution clef en main pour des missions temporaire mais inexploitable pour une solution a long terme car on a pas autant de liberté qu'avec une solution Nagios/Centreon « normale »

Remarque : La FAN est composé de Nagios, Centreon, Nagvis et Nareto mais nous intéresseront seulement à nagios et à Centreonce projet et nous donnerons une rapide présentation du troisième.

En ce qui concerne l'installation de la FAN, nous l'avons réalisé sur une de nos machines qui était relié au réseau de Candide SA. Nous avons convenu plusieurs rendez vous afin d'installer les plugins sur les diverses machines clientes.



Architecture de supervision

Nagios

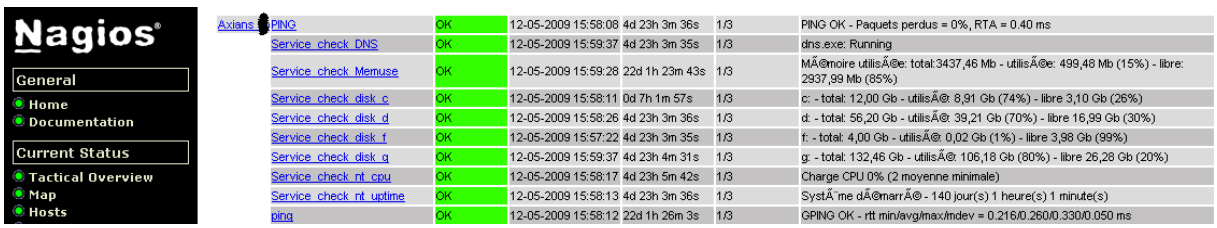
Nagios (anciennement appelé Netsaint) est un outil qui permet **de nous alerter en temps réel lorsqu'un problème survient et de manière graphique grâce au greffon Centreon**. Centreon permet aussi de gérer les fichiers de configuration, car il faut savoir que Nagios ne se configure qu'en ligne de commande. Les différentes machines et services sont surveiller grâce a des plugins, encore appelé module d'extension sont des programmes externes. Certains d'entres eux sont intégrés de base (smtp, ping, web,…).

Nagios surveille les hôtes et services que l'on spécifie, pous alertant lorsque les systèmes vont mal et quand ils vont bien. C'est un logiciel libre sous licence GPL (General Public License). Il est donc totalement gratuit, et fonctionne uniquement sous Linux.

C'est un programme modulaire qui se décompose en trois parties :

- Le moteur de l'application, qui vient ordonnancer les tâches de supervision ;
- L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies ;
- Les modules d'extension ou plugins, une centaine de mini programmes, que l'on peut compléter en fonction des besoins de chacun pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du SI.

L'outil libre de monitoring réseau est passé en version 3.0 récemment. Nous avons donc installé cette nouvelle monture sous le système d'exploitation Debian. Nous avons installé un serveur web et les librairies de bases nécessaires pour la compilation de Nagios.



Interface Nagios

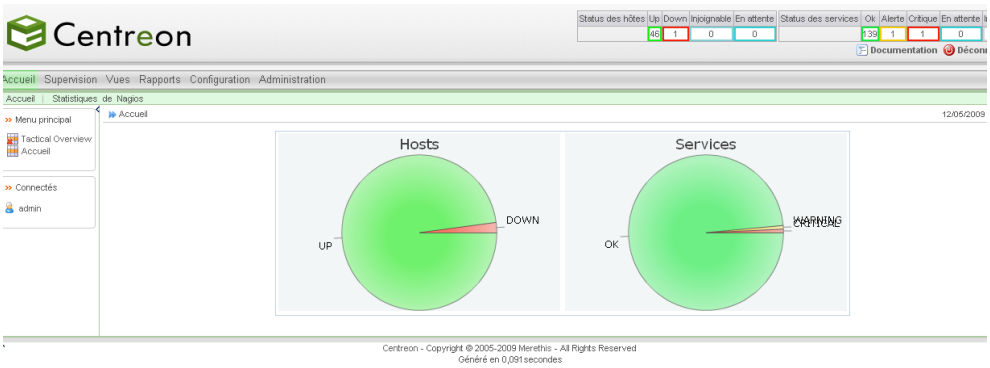
Centreon

Centreon (anciennement Oreon) **est une surcouche applicative de Nagios**. C'est un logiciel libre sous licence GPL.
Il a été développé par une équipe Française. **Centreon permet de configurer Nagios via une interface web.** En effet, le gros problème de Nagios est la configuration des hôtes et services. Sous Nagios, toute la configuration se réalise avec plusieurs fichiers de configurations. On doit écrire ligne par ligne chacun des hôtes et services, ce qui peut impliquer beaucoup de temps suivant le nombre important d'équipements à superviser.

Centreon permet de résoudre cette lacune tout en gardant les fonctionnalités du moteur de Nagios. Il gère également des modèles d'hôtes et de service, ce qui permet de dupliquer très rapidement les machines concernées. Ainsi, Le gain de temps avec Centreon

est conséquent. Il permet de plus de générer automatiquement les fichiers « textes » de Nagios. Il ne reste par conséquent que l'écriture ligne par ligne à effectuer.

De plus, **l'interface graphique proposée par Centreon est plus agréable que celle de Nagios**, et entièrement francisée. Les données sont également **mieux interprétées par Centreon**, ce qui lui permet de proposer des graphiques beaucoup plus détaillés que sous Nagios.



Interface Centreon

Les plugins

Les plugins sont des programmes exécutables ou script (perl, shell,…) capables de fournir au moteur :

- Un code de retour :

- Et un court message descriptif

Le code de retour est différent selon le seuil définit par l'administrateur. On définit 3 seuils par :

Plugin : le seuil « **OK** », le seuil «**Warning** », et le seuil « **Critical** ».

Par exemple, lorsqu'on vérifie la CPU d'un serveur, on peut définir 2 seuils :

- le seuil **Warning** à 80%
- le seuil **Critical** à 90%.

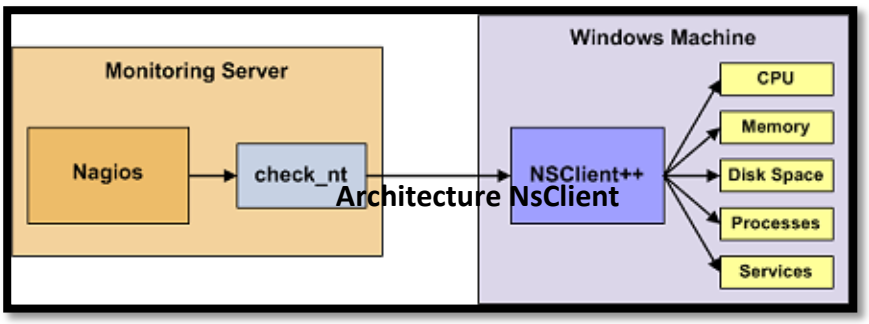
Dès lors qu'un serveur dépasse 80% de charge CPU, Nagios émettra une alerte **Warning**, et une alerte **Critical** à 90% d'utilisation de CPU.

Il existe principalement deux types de plugins destinés aux serveurs, pour les serveurs Windows (nsclient ++) et les serveurs linux (nrpe). En effet, notre objectif était de superviser différents éléments sur les serveurs comme par exemple, la charge CPU, les

processus actifs… Afin de procéder à l'installation des plugins sur les machines de Candide SA, nous avons pris rendez vous avec eux afin de réaliser les différentes configurations.

Pour les systèmes Windows : NsClient

Le plugin utilisé pour le système Windows est appelé « Nsclient++ ». Il n'utilise pas le protocole de supervision SNMP. En fait, il utilise ses propres données puisque le système est un système Client-serveur, comme le montre le schéma ci-dessous :

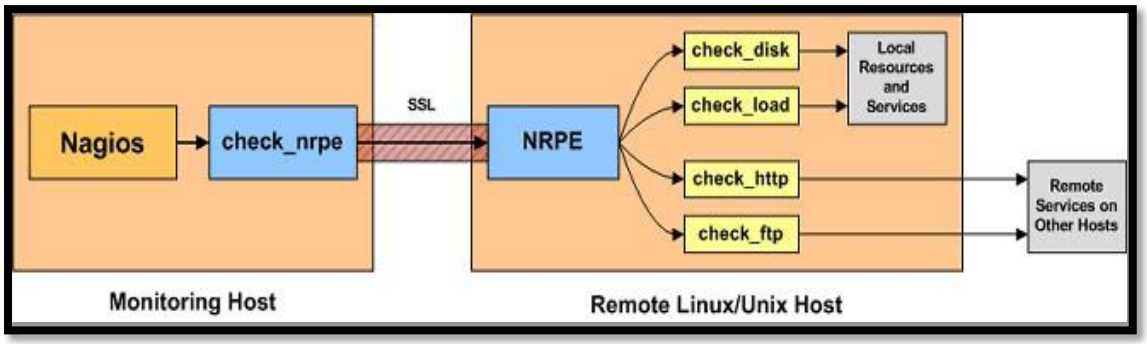


Architecture NsClient

C'est un plugin qui permet de récupérer un nombre important d'informations. Il faut tout d'abord savoir que le logiciel Nsclient ++ est destiné aux machines Windows. Il existe également un plugin destiné aux machines linux, présenté si dessous. La partie cliente (nommée **check_nt**), doit être présente sur le serveur Nagios. La partie serveur (**Nsclient++**) est à installer sur chacune des machines Windows à surveiller. Ce plugin permet de retourner de nombreuses informations telles que la charge de la CPU, la mémoire utilisée, ou encore l'espace disque…).

Pour les systèmes linux : NRPE

Afin de mettre en place une supervision de machine Linux, il est nécessaire d'utiliser le plugin NRPE. Le principe est le suivant :



Architecture NRPE

Il est nécessaire de modifier les deux équipements, la machine hébergeant Nagios ainsi que les machines Linux à surveiller. Il faut aussi installer le démon NRPE sur la machine hôte Linux seulement. Afin de communiquer les deux machines utilisent un tunnel SSL pour crypter les informations. Une installation d'openSSL (logiciel libre pour SSL) est donc indispensable sur les deux équipements.

En résumé:

- Nagios appelle son plugin check_nrpe ;
- Ce dernier via un tunnel SSH contacte le démon NRPE sur la machine distante
  - Linux ;
- NRPE récupère les informations voulues par ses différents plugins ;
- NRPE renvoie ces informations à Nagios.

Remarque : *Il est possible de ne pas utiliser SSL pour le lien entre les machines grâce à une option du plugin check_nrpe.*

c. L'outil CACTI

CACTI est un outil de surveillance basé sur le célèbre RRDTool, permettant de connaître toutes les données systèmes des ordinateurs du réseau. Il les présente automatiquement sous forme de graphiques consultables depuis une page web. Par ailleurs, il dispose d'un système de plugins qui le rend simple d'utilisation et très modulaire.

Il est ainsi possible de le coupler à GLPI ou NAGIOS afin de disposer d'un outil de gestion pour le parc.

La surveillance d'un système permet de connaître sa disponibilité à un instant T, mais aussi de mesurer dans le temps l'évolution d'un certain nombre de paramètres tels que l'occupation de l'espace disque ou la charge mémoire. Il devient alors possible par extrapolation de prévenir le moment de rupture du système en prenant des mesures préventives. CACTI utilise également une base MySQL pour stocker la configuration. L'interface est divisée en deux, une partie nommée "Console" permettant de tout configurer et une autre nommée "Graphs" permettant d'afficher les graphiques. L'originalité réside dans le fait que la partie affichage de graphiques possède trois modes d'affichages :

- **Tree mode** : Classement en arbre des différentes machines par groupes.
- **List mode** : Permet de lister les graphiques présents sur une machine sélectionnée.
- **Preview mode** : Ressemble à List Mode excepté que les graphiques sont affichées directement au lieu d'un lien vers celui-ci. Utile pour avoir un aperçu rapide de l'état d'une machine et de ses services.

CACTI relève l'ensemble des données toutes les 5 minutes. On crée ensuite des graphes associés aux données. Les graphes sont produits à la demande. Pour faciliter la configuration, les types de données, les graphes et les équipements à monitorer sont stockés sous forme de modèle (template). On définit d'abord les sources de données. Elles seront obtenues par SNMP ou via un script. Il faut bien entendu installer et configurer les agents SNMP sur les stations et serveurs à surveiller.

Ajout de plugins pour étendre les fonctionnalités à CACTI:

Par exemple, l'implémentation du plugin syslog-ng permettant de lire les messages syslogs dans l'interface web de CACTI.

Les programmes suivants sont requis pour faire tourner CACTI:

- apache2 pour le serveur web
- mysql-server pour la base de données
- php5, php5-common, php5-cgi, php5-cli, php5-mysql pour le language de script nmp - pour collecter les statistiques SNMP des agents distants. rrdtool - un script pour formater les données colléctés en fichier rrd.

Avantages

- Interface très claire
- Configuration facile avec l'utilisation des templates pour les machines, les graphiques, et la récupération des données tout se configure aisément et entièrement via l'interface web. Import/ Export très simple des templates au format XML.
- Performance : Choix du moteur de récolte des données permettant d'opter pour la performance ou la simplicité
- Gestion des utilisateurs
- Notoriété sur le web, présence d'une dizaine de plugins permettant d'étendre les fonctionnalités

Inconvénients :

- Pas de gestion d'alarmes, sauf avec un plugin nommé Thold.
- Pas de gestion de panne et absence d'une cartographie de réseau.
- Configuration au clic, pas de fichier texte à éditer

Conclusion :

Nos tests nous ont montré que Cacti est vraiment un outil complet permettant d'avoir grâce aux différents graphes et plugins des aperçus rapide de la situation du réseau, des services, des serveurs…

d. L'outils MBSA (Microsoft Baseline Security Analyser)

Candide SA ayant une architecture Active Directory 2003, il nous a donc semblé intéressant d'avoir un outil spécialement conçu pour **les architectures Microsoft**. Il existe un outil d'analyse de sécurité nommé **MBSA.** Cette outils permet d'analyser, de surveiller et de remédier aux problèmes de sécurité connus des produits Microsoft tels que les systèmes d'exploitation Windows XP, Windows Server 2003, Windows 2000 et les applications courantes (Internet Explorer, Outlook Express, Lecteur Windows Media, Office, IIS, SQL Server, Exchange Server, Microsoft Data Access Components, MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server et Host Intégration Server). Cet outil permet donc d'avoir une vision globale de la sécurité de l'infrastructure Microsoft déployée.

Il faut ensuite sélectionner les options d'analyse, choisir les éléments à analyser en cochant les cases des options que vous désirez :

Les différentes options d'analyse sont:

- Vérifications des vulnérabilités administratives du système.
- Vérification des mots de passe vulnérables.
- Vérifications des vulnérabilités administratives des services IIS.
- Vérifications des vulnérabilités administratives de SQL Server.
- Vérification des mises à jour de la sécurité : Windows NT 4.0, 2000, XP et Server 2003, Services IIS 4.0, 5.0 et 6.0, SQL Server 7.0, 2000 Internet Explorer 5.01 et +, Media Player 6.4 + , Exchange Server 5.5, 2000 et 2003, MDAC 2.5 et +, , Machine virtuelle Microsoft, MSXML 2.5, 2.6, 3.0 et 4.0, Content Management Server 2001 et +, Commerce Server 2000 et +, BizTalk® Server 2000 et +, SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004, Office.

Exemple de résultats

Après quelques minutes d'analyse, le rapport de sécurité est affiché. La première partie du rapport nous donne l'évaluation de la sécurité du pc (risque important, risque faible, ...) :

La seconde partie indique le niveau de sécurité par catégorie (Office, Windows, ...) et le nombre de mises à jour de sécurité manquante :

La croix rouge indique qu'il manque des mises à jour critiques, la croix jaune qu'il manque des mises à jour non critiques et le V vert indique que tout est OK.

Conclusion :

L'utilisation de MBSA a elle aussi été compliqué dans la mesure où l'architecture active directory 2003 n'a quasiment jamais été fonctionnelle. (Les utilisateurs n'étaient pas loguer sur le domaine 2003). Cependant il reste un très bon outil pour détecter les failles des produits Microsoft.

e. NetFlow

La défense a utilisé un routeur Cisco et un routeur BSD dans son infrastructure. Nous leur avons donc demandé de nous faire remonter les informations des routeurs via Netflow.

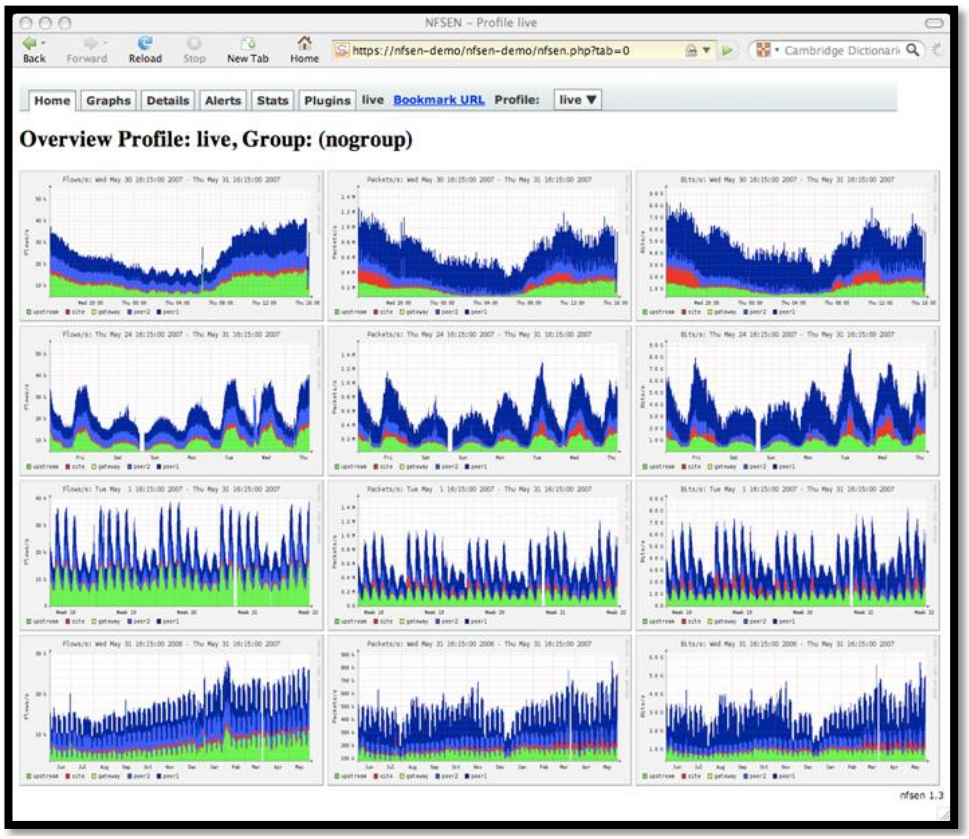
Nous avons opté pour **la partie monitoring au couple de logiciels nfdump et nfsen :**

- **Nfdump** s'occupe d'enregistrer les informations remontées par les routeurs.
- **Nfsen** s'occupe du rendu et de la présentation des statistiques via une interface Web.

Les informations récoltées sont intéressantes dans le cadre du monitoring puisqu'on a des compteurs par type de trafic et par port, ce qui permet de constater une activité suspecte.

Le problème de ces solutions, c'est qu'elles ne permettent pas de base de faire un recoupement. Ce qui permettrait d'identifier avec certitude l'activité suspecte.
Cette solution fait partie des classiques pour le monitoring. Nous pensons qu'elle devrait être mise en place sur le long terme par l'équipe défense.

Pour un audit sur une courte période, **ne pas avoir de base de comparaison est un réel handicap pour détecter une activité « anormale »**.



f. L'outils ZABIX

Présentation

ZABBIX Zabbix est un logiciel de supervision distribué Open Source créé par Alexei Vladishev. Il permet de surveiller des périphériques au sein d'un parc informatique.

Fonctionnalités

Zabbix offre en autre les possibilités suivantes :

- Monitoring distribué
- Monitoring en temps réel
- Scalabilitté
- Visualisation de l'activité via des graphes
- Outils de reporting (log)
- Auto découverte des éléments réseaux
- Flexibilité (multi-plateforme, support de l'IPV4 et IPV6
- Monitoring des stations sans agent
- Importation et exportation de données XML (template)
- …

Pré requis matériel

Resource	Minumum	Recommended
Disk space	10 MB	100 MB
RAM	64 MB	256 MB
CPU	Pentium	Pentium IV or equivalent

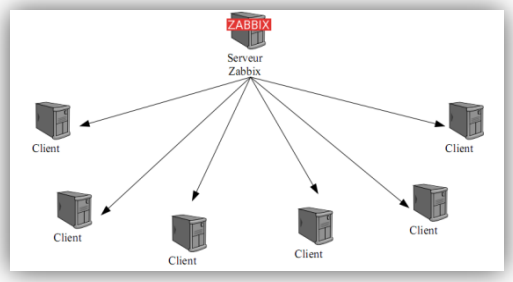
Os supportés

Platform	ZABBIX Server	ZABBIX Agent
AIX	Supported	Supported
FreeBSD	Supported	Supported
HP-UX	Supported	Supported
Linux	Supported	Supported
Mac OS X	Supported	Supported
Novell Netware	-	Supported
Open BSD	Supported	Supported
SCO Open Server	Supported	Supported
Solaris	Supported	Supported
Tru64/OSF	Supported	Supported
Windows NT 4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista	-	Supported

Différents types d'utilisation

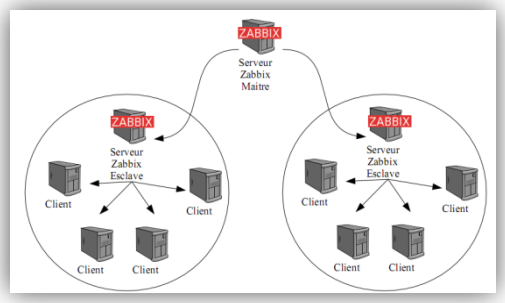
Collecte simple

Dans ce cas Zabbix va récolter les informations de ses clients sans passer par l'utilisation d'agents.



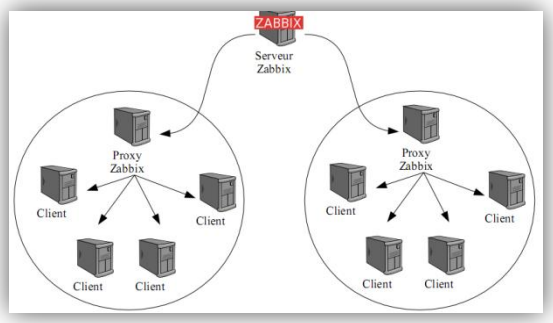
Serveurs Distribués

Ce modèle d'utilisation a été implémenté dans la version 1.4 de Zabbix. Dans un premier temps on déclarait un serveur maître et ensuite des serveurs esclaves. Ces derniers récupéraient les informations des clients et ensuite les renvoyaient au serveur maître.



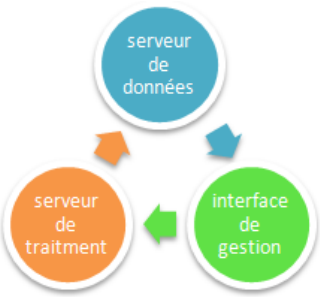
Collecte distribuée

Ce modèle est implanté dans la version 1.6 de Zabbix, elle permet aux clients d'envoyer les informations des clients via un serveur de base de donnée vers le serveur Zabbix.



Principe de fonctionnement

Le "serveur ZABBIX" peut être décomposé en 3 parties séparées



Le serveur de données

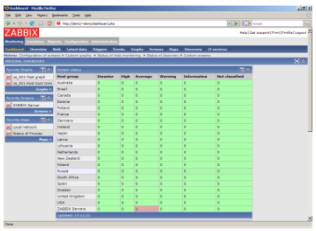
Zabbix, comme la majorité des outils de supervision, repose sur une base de données pour pouvoir stocker les informations. Selon l'importance du nombre de

machines et de données à surveiller, le choix du SGBD influe grandement sur les performances. Il est notamment possible d'utiliser Zabbix avec MySQL ou Oracle.

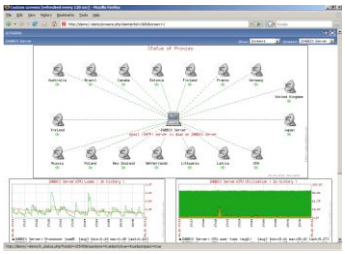
L'interface de gestion

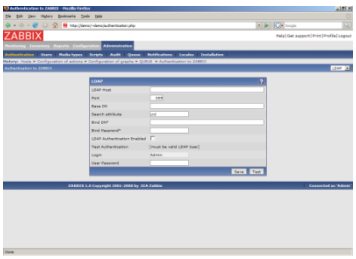
Son interface web est écrite en PHP. Elle agit directement sur les informations stockées dans la base de données. Chaque information nécessaire au serveur de traitement étant réactualisée automatiquement, il n'y a pas d'action à effectuer sur le binaire pour lui indiquer qu'il y a eu une mise à jour.

Cette interface dispose des fonctionnalités principales suivantes:



- Affichage des données et état des machines
- Génération de graphiques (évolution des données et état des machines/liens)
- Classement et groupement des machines surveillées
- Auto découverte de machines et ajout automatique
- Gestion fine des droits d'accès pour les utilisateurs de l'interface





Le serveur de traitement

Le serveur de traitement est en fait un démon binaire. Il offre diverses options de monitoring. La vérification simple permet de vérifier la disponibilité ainsi que le temps de réponse de services standards comme SMTP ou HTTP sans installer aucun logiciel sur l'hôte monitoré. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque... Le logiciel peut réaliser le monitoring via SNMP.

Lexique

ZABBIX se distingue d'autres produits de supervision par un lexique bien particulier :

Trigger

Un trigger déclenche une alarme suite à un événement défini *via* une expression. ZABBIX dispose d'une liste de *triggers* prédéfinis, et modifiables. Par exemple :

- le trigger "Low free disk space on Debian volume /home" (espace disque insuffisant sur le serveur Debian volume /home),

Item

Un item est un élément à vérifier ou à superviser (charge du processeur, mémoire libre etc.). Il est possible de créer son propre item. Chaque item est créé avec une ou plusieurs clés, qui sont des fonctions retournant une valeur mesurée. Par exemple :

- L'item "Total disk space on /home" a pour clé vfs.fs.size[/home,total].

Action

Une action est en fait un traitement effectué en cas de déclenchement d'alarme. Une action peut servir à pallier un éventuel problème, ou simplement à prévenir une personne. Exemple d'actions :

- l'envoi d'un mail,
- une commande à exécuter.

Template

Un template est un modèle pouvant être créé et chargé dans ZABBIX. Un template peut contenir :

- des *items*
- des *triggers*
- des graphes personnalisés, etc.

Comparaison ZABBIX et Nagios

Si l'on compare ZABBIX et Nagios, on constate les différences et les particularités suivantes :

- Nagios permet de tester l'état de service un certain nombre de fois avant de considérer qu'il y a défaillance et de remonter l'alerte. ZABBIX n'offre pas cette possibilité.
- Le système d'alerte de Nagios est plus robuste, et plus simple à mettre en place que celui de ZABBIX.
- Les rapports et les fonctionnalités graphiques offerts par ZABBIX sont nettement plus riches et plus synthétiques que ceux de Nagios. Pour arriver à un résultat équivalent, Nagios devrait être couplé à un autre outil comme Cacti, Munin ou Centreon.
- ZABBIX se distingue de Nagios par une interface web riche d'administration, qui permet la configuration de tous les paramètres de supervision (services, hôtes à superviser, etc.). La configuration avec Nagios se fait à la main en éditant directement des fichiers textes.
- ZABBIX est plus orienté vers la mesure des données de performances. Nagios est davantage orienté vers la mesure des données d'état.

Conclusion :

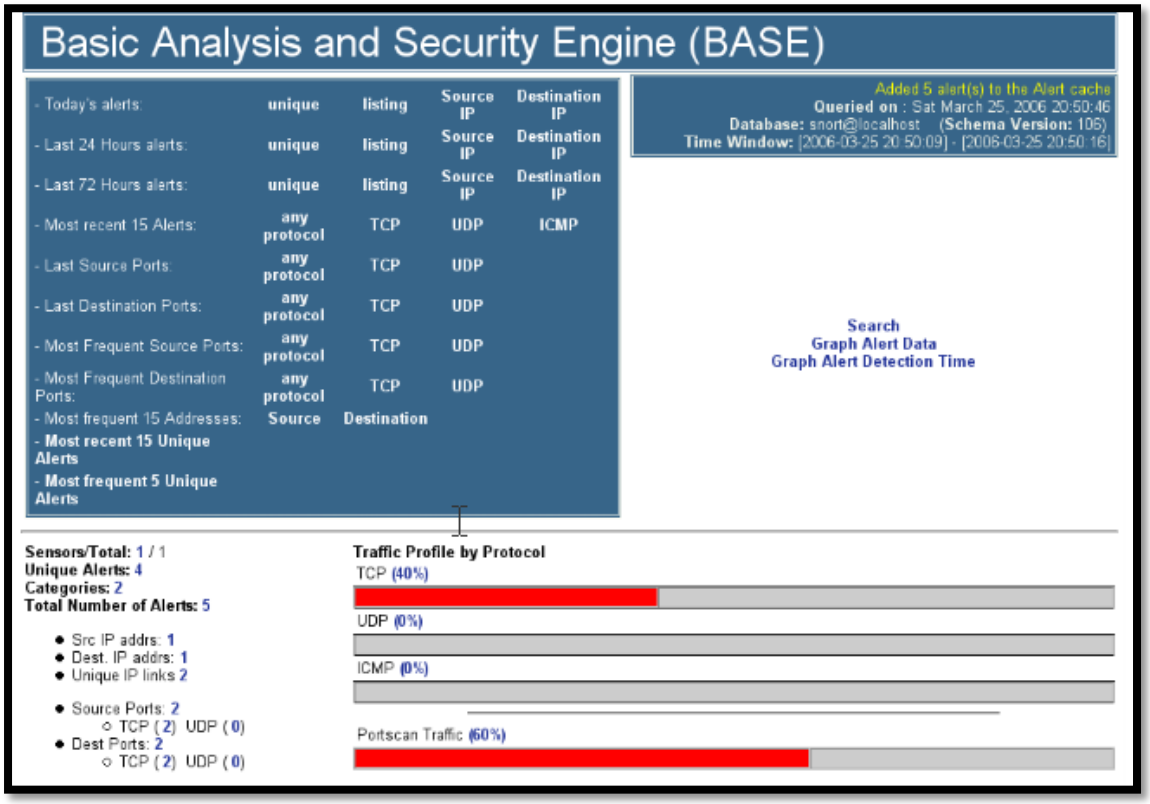
ZABBIX est un puissant outil de *monitoring*, facile à mettre en œuvre et à paramétrer. Il se pose en outil équivalent à Nagios. Employer ses deux outils simultanément sur un parc nous semblerait inutile car les fonctionnalités sont équivalentes. Notre préférence ira tout de même vers Nagios qui nous semble plus complet malgré la richesse de Zabbix.

g. *Le logiciel BASE*

Base est le logiciel le plus en vogue actuellement. Il est issu d un projet open-source basé sur ACID (Analysis Console for Intrusion Databases). La console BASE est une application Web écrite en PHP qui interface la base de données dans laquelle Snort stocke ses alertes. Pour fonctionner, BASE a besoin d'un certain nombre de dépendances :

- Un SGBD installé, par exemple MySQL
- Snort compilé avec le support de ce SGBD
- Un serveur HTTP, par exemple Apache
- L'interpréteur PHP avec les supports pour le SGBD choisi, la bibliothèque GD et les sockets.
- La bibliothèque ADODB : http://adodb.sourceforge.net

Après installation nous pouvons obtenir ceci :



h. L'outil AlienVolt

Présentation générale

Alienvault OSSIM (Open Source Security Information Management System) se présente sous la forme d'une interface graphique regroupant plusieurs composants Open Source. Les objectifs de cette solution sont :

- Fournir une interface graphique d'administration
- Donner accès à une plate-forme remontant des événements de sécurité
- Effectuer une analyse de corrélation afin de créer des alarmes de sécurité à partir de plusieurs événements remontés par les sondes

En ce qui concerne l'architecture, elle est composée d'un serveur centralisé sur lequel des agents peuvent se connecter.
En effet OSSIM met en jeu 2 processus appelé **Ossim-Agent** et **Ossim-Server** dont voici les caractéristiques.

- **Ossim-agent** héberge les différents plugins (sonde réseau, sonde de statistiques réseaux, etc..). L'agent récupère ensuite les informations des fichiers de logs des plugins et les envoie directement au serveur OSSIM permettant ainsi le traitement en temps réel des informations. L'agent OSSIM s'occupera aussi de la mise en marche et de l'arrêt des différentes sondes (plugins) qu'il héberge. Il ne sera ainsi pas nécessaire de démarrer les plugins des agents à la main puisque leur activation sera effectuée depuis la console de management offerte par Ossim-server.

- **Ossim-server** constitue le noyau de l'architecture. En effet, celui-ci contient les modules d'analyse et de corrélation des données ainsi qu'un serveur Web permettant l'interaction avec l'utilisateur (administrateur réseau en charge de la sécurité).

Outils de communication et sécurisation des outils

Le groupe Audit a **mis en place « Alienvault » pour la dernière confrontation**. C'est un outil très intéressant étant donné que plusieurs fonctionnalités sont déjà préconfigurées et que son installation est relativement simple.

Voici maintenant quelques unes de ces principales fonctionnalités présentes dans le tableau de bord général de « Alienvault »:

- « Executive » : Informations générales sur l'ensemble du réseau (Niveau d'alerte, Alarmes et événements, Top10 des risques, carte de disponibilité du réseau, etc.).

- « Tickets » : Système utilisé lister les incidents.

- « Security » : Répertorie toutes les alarmes qui ont été déclenché dans un tableau (avec les données suivantes : type d'alarme, niveau de risque, source IP, destination, etc.).

- « Network » : Représente des statistiques générales sur le trafic du réseau (trafic, paquets,etc.).

- « Inventory » : Détails des statuts des applications installés, des processus en cours et aussi du matériel informatique.

- « Vulnerabilities » : Vues détaillées des résultats des rapports sur les scans de vulnérabilités. On peut y voir les failles de sécurités ainsi que les recommandations pour les résoudre.

- « Compliance » : Graphes sur la mesure de la sécurité par rapport à la norme ISO 2700X.

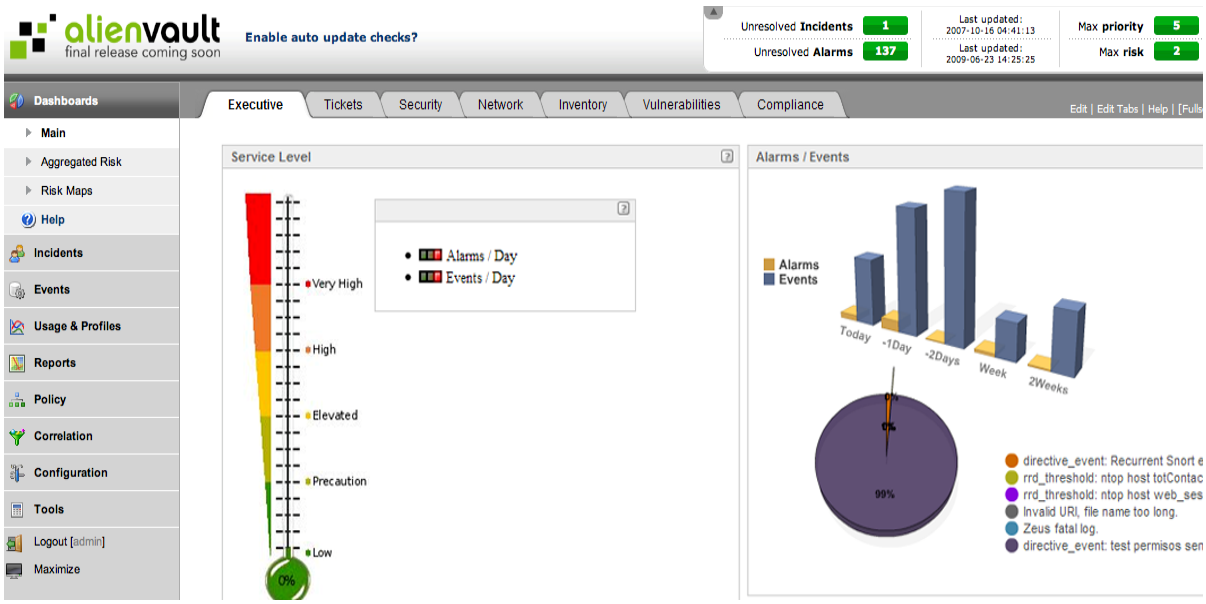


Tableau de bord du réseau

Conclusion :

Avantages : Alienvault OSSIM se révèle être une solution proposant des concepts d'analyses très innovateurs. En effet, peu de solutions Open Source proposent actuellement une telle palette de procédés d'analyse d'événements de sécurité:

- Récupération d'événements d'infrastructures hétérogènes (alertes de NIDS, logs, etc...).
- Attribution d'une sévérité à chaque événement en fonction de l'attention que l'on porte au bien potentiellement attaqué (priorization des alertes).
- Corrélation croisée (Nessus - Snort) permettant la modification de la sévérité des alertes en fonction des vulnérabilités de la cible de l'attaque potentielle.
- Analyse comportementale du réseau permettant la génération d'alertes en fonction du comportement des utilisateurs (Ntop et l'algoritme Holt-Winter de RRD).
- Corrélation des événements et intégration des événements de l'analyse comportementale dans ce procédé.

Inconvénients : La configuration de cette solution reste fastidieuse. Cela est du au grand nombre de paramètres qui peuvent rentrer en jeu. De plus, elle ne peut pas être déployée sur le long terme car elle consomme beaucoup de ressources à cause de tous les utilitaires qui tournent, et ne peut donc passer l'échelle sur un réseau chargé. Nous émettons des réserves sur le matériel vendu par la société, certains outils nécessitent une machine dédiée.

4. Conclusion

Ces différents logiciels sont des incontournables pour une infrastructure qui souhaite avoir un suivi et un œil sur l'activité de son réseau.
Les résultats pris de manière isolée n'apportent pas grand-chose pour identifier clairement la cause de l'activité (version x du virus y par exemple).
Les solutions proposées à l'heure actuelle ne proposent pas pour l'instant de se baser sur ce type de recoupement pour détecter une intrusion à priori, et ne se basent que sur des empreintes pour une détection à posteriori.
Cependant, en présentant les différents graphiques sur une même page, on pourrait déjà recouper de manière « manuelle » différents marqueurs, mettant en avant la compromission d'une machine.

V. Le mode "ATTAQUE"

Il n'est pas rare d'entendre que telle entreprise à subit un vol de données, un commercial s'est faits volé son ordinateur portable, et entraine le plus souvent une perte pouvant se chiffrer en millions pour un opérateur ou en suicide commercial dans un centre de R&D. C'est donc dans ce contexte et suite à une analyse que nous avons pu mener en observant l'équipe défense au quotidien que nous avons décidé de simuler des attaques. De plus, Les tests d'intrusion consistent à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle. Il s'agit d'audit actif.

1. Le virus conficker

Objectif :

Etudier l'implémentation d'un confliker au sein de l'entreprise Candide SA

Le matériel utilisé :

- 2 machines virtuelles sous Windows XP SP3.
- 1 machine virtuelle pour la supervision des machines.

Installation du parc :

Afin de coller au mieux à la réalité du parc à superviser, nous avons demandé à la société Candide S.A de nous fournir deux ISO de leurs machines clientes afin de déterminer leur réaction lors de l'infection.

Nous avons décidé d'utiliser la virtualisation pour l'installation du parc informatique. Ainsi nous pouvons couper le parc en cas de dérive liés à l'implémentation du confliker.

Installation de l'outil de supervision :

Pour pouvoir analyser l'impact du confliker ainsi que la réaction de chaque machine nous avons de choisis de mettre en place plusieurs outils de supervision (tels que ACID, netflow, nmap, Nagios). Ces derniers étant déjà mis en place sur le parc Candide SA et en fonctionnement nous avions décidé de se tourner vers une distribution dénommée « alienVolt » pour ne pas corrompre le bon fonctionnement de ces outils.
Tous comme les machines clientes nous avons décidé de l'installer sur une machine virtuelle grâce à l'outil KVM
Après l'installation de ces trois machines nous pouvons commencer l'analyse du Confiker.

Pourquoi choisir ce type d'attaque :

Récemment dans l'actualité de nos medias favoris on pouvait lire : « Nouvel arrivé, le vers Confiker, qui a déjà contaminé des millions d'ordinateurs dans le monde. S'ils se réveillaient tous en même temps, ils pourraient constituer un réseau d'attaques massives,

une perspective digne d'un scénario catastrophe, envisagée par la plupart des éditeurs d'antivirus ». Ou encore « un virus exterminateur ».
C'est donc dans ce contexte un peu nouveau que nous avons choisi de faire une simulation pour voir l'impact de ce virus sur le parc informatique si une infection venait à survenir.

Comment fonctionne le Confiker C ?

Fonctionnement global :

Voici une image très simpliste du fonctionnement du confiker.

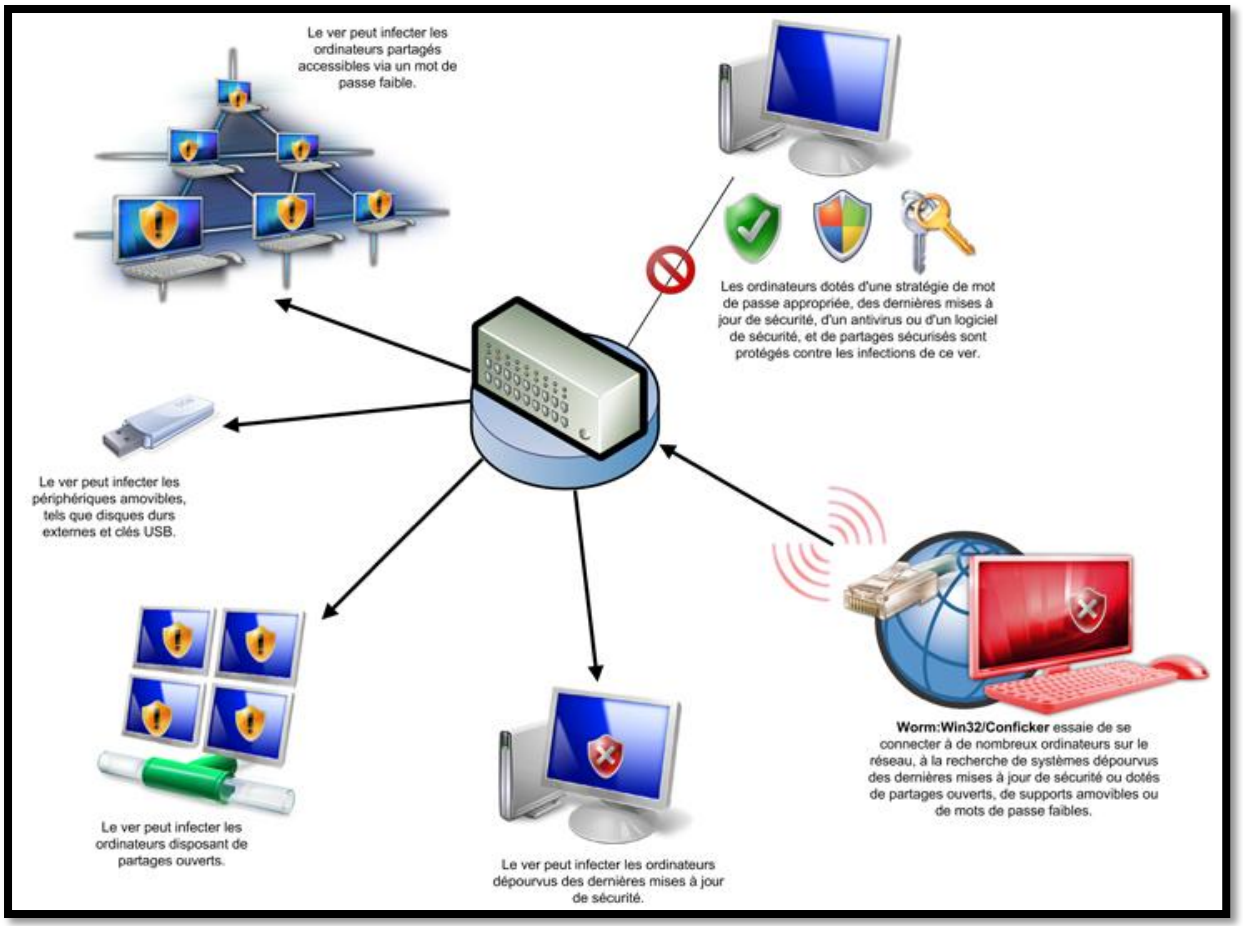
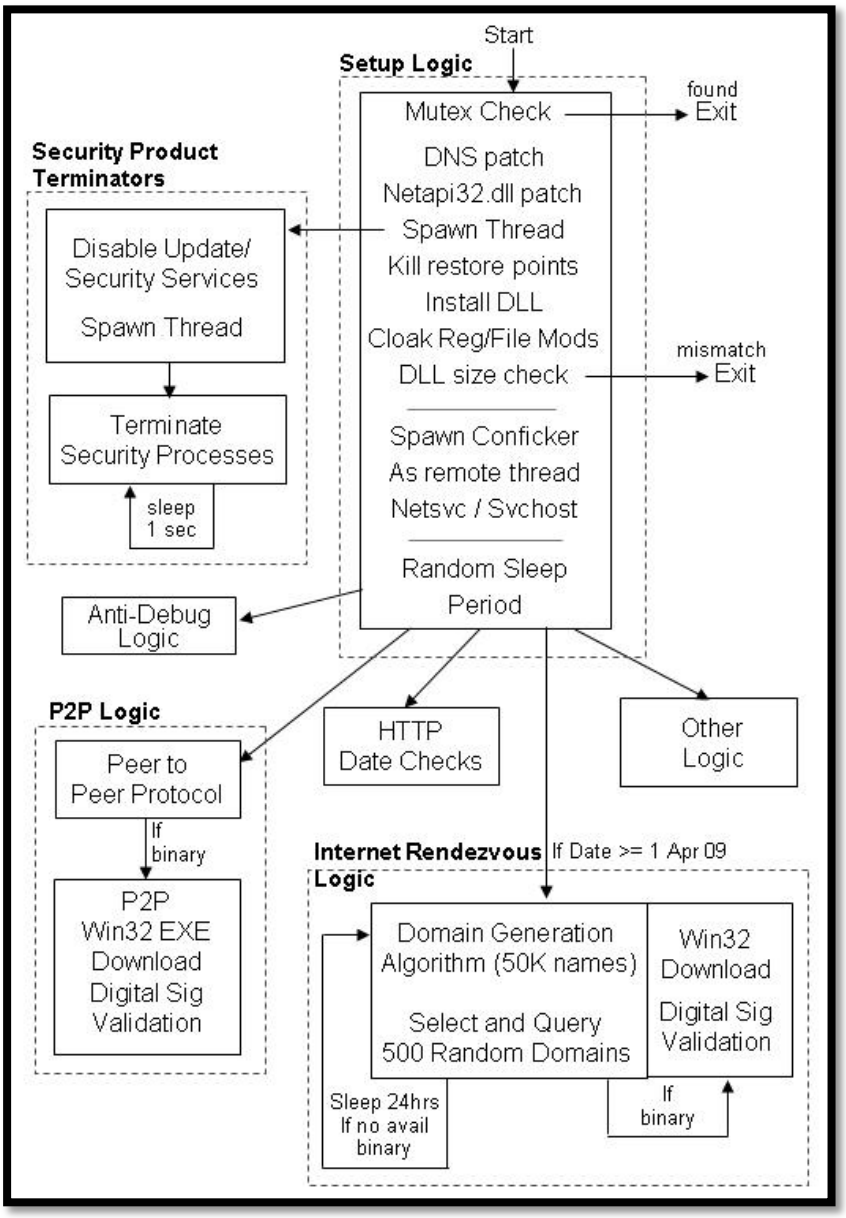


Figure 1- fonctionnement Confiker- sources: microsoft.com

Sur cette image on s'aperçoit très simplement que un ordinateur d'un particulier ou bien d'un hacker possédant le Virus va le rependre sur l'internet. Ce dernier va chercher à s'introduire sur n'importe quel medias qui sont dépourvus de mise à jour de sécurité ou bien encore disposant de partages ouverts et même découvrir des mots de passe faible.
Après avoir vu le fonctionnement de manière très globale du virus nous allons nous intéresser au fonctionnement logique de ce dernier.

Fonctionnement logique :

Afin de mieux comprendre le fonctionnement nous vous proposons ce schéma.



La première étape réalisée par le virus lorsqu'il rentre sur un media est de vérifier si il n'est pas déjà infecté ceci est réalisé par un test sur une DLL.
A l'intérieure de la DLL il vérifie la présence de trois valeurs mutex sur l'hôte cible pour éviter une réinfection.

En cas d'absence, ces trois mutex sont créés:

- Le nom mutex "Global \ <string> -7",
- Le nom de mutex "Global \ <string> -99
- Un mutex nommé pseudo-aléatoire basé sur l'ID de processus.
  Le <string> dans les deux premiers mutex est unique par ordinateur, il est calculé sur la base du hachage crc32 du nom d'ordinateur et XOR'ed avec une constante. Puis il installe plusieurs correctifs en mémoire, et incorpore d'autres mécanismes

pour contrecarrer les applications de sécurité qui, autrement, détecteront sa présence.

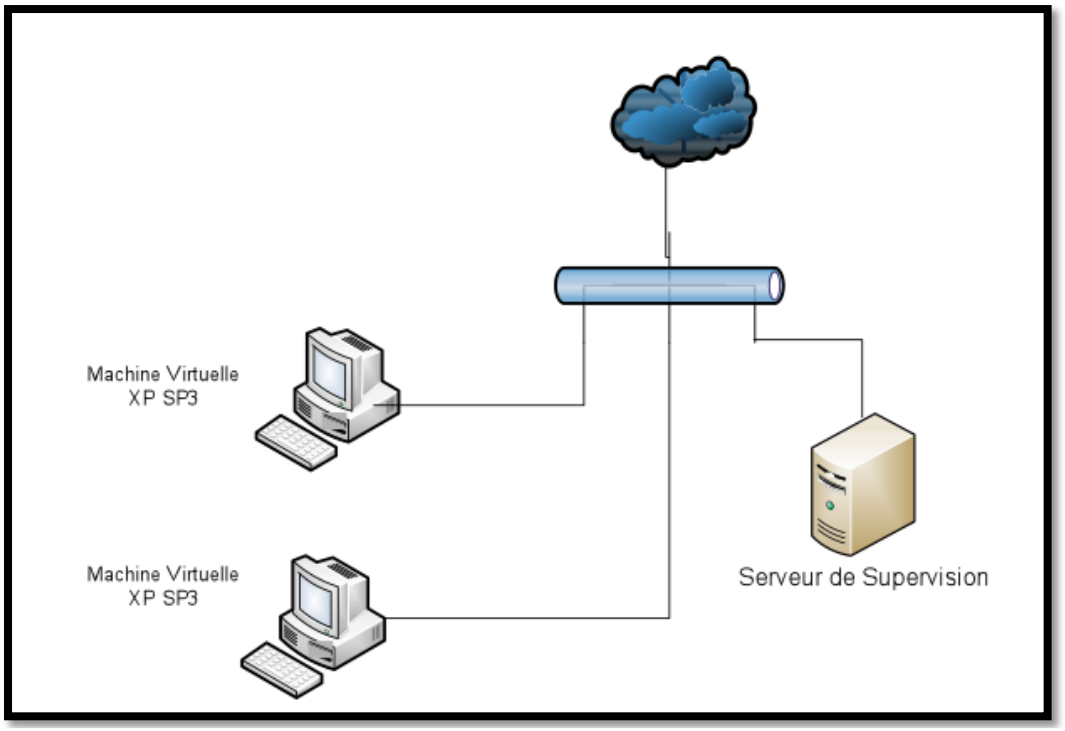
Ensuite il modifie le DNS et les API de sécurité pour bloquer les diverses connexions de réseau connexes (Domain Lookup Prévention), et installe un pseudo-patch pour réparer la vulnérabilité 445/TCP, tout en maintenant un moyen détourné d'une réinfection (Local Host Patch Logic).

Ce « pseudo patch » protège l'hôte à partir des dépassements de tampon par des sources autres que celles exercées par les auteurs Conficker ou de leurs pairs infectés.
Ensuite Confiker va crée un Thread dont le but principal est de désactiver les processus de sécurité interne au PC tels que Windows Defender, ainsi que Windows Update. Pour finir il désactive le mode safeboot présent comme option au redémarrage d'un PC.
Dans cette situation actuelle, le PC infecté n'est plus protégé et le confiker c'est bien installé.
Le virus va finir son installation en mettant à jour sa DLL, en récupérant la date fixée dans l'kernel32.dll sans crainte d'être supprimé puisqu'aucun système antivirus ne peut le détecter car ces derniers sont désactivés.
Une fois l'installation terminée, la DLL crée un thread distant, qui s'attache au processus de netsvcs.exe ou svchost.exe, selon la version OS.

Par la suite le Confiker va aller modifier l'algorithme de génération de domaine et va activer à la date du 1 avril 2009 un processus pour qu'il se rend actif a cette date ;
A cette « deadline » le confliker aura pour rôle de créer un réseau parallèle qui fonctionne en P2P sur 2 ports TCP et UDP.
Les premiers résultats sur des opérations en milieu infecté contrôlé, montrent que confiker.c lance des tentatives de connexions TCP sur seulement 60 hosts toutes les 5 minutes, jusqu'à 2500 hosts en UDP dans la même période de temps, et 6 connexions http sur des serveurs qui pourraient contenir de nouveaux exploits à télécharger. Répète l'action ainsi de suite sur les machines infectées.

L'inconvénient de ce type de virus est qu'il multiplie les défenses et est quasiment ineffaçable. En effet comme on l'as vu dans la toute première partie il utilise les MUTEX ceci induit qu'il est presque impossible à détruire le process en ram. De plus il verrouille les outils de reverse engineering et utilise également le cryptage de répertoire et données en MD6.Il utilise aussi la techniques de compétences transversales afin de tester si la machine, qui est en cours d'infection, a déjà été touchée par une ancienne version de confiker. Si oui, le process se connecte sur la machine déjà infectée par une version antérieure a la variante C, l'update en version C, avec mise à jour ou création d'une DLL dans un répertoire temporaire crypté en MD6. La dll s'exécute par svchost, lance des requêtes sur des DNS defacés via un « DNS changer ».
Après avoir analysé de façon très théorique l'installation du confliker, nous avons souhaité voir son impact réel sur un réseau virtuel censé représenter une partie du parc de la société.

L'installation :



Les deux machines virtuelles sont installées sous KVM.
Le Serveur de supervision est virtualisé sous Wmare et utilise le logiciel AlienVolt.

Comment récupérer le Conflicker.C ?

Dans un premier temps, nous avons pensé trouver les sources sur internet. Mais ceci c'est révélés un échec. Effectivement il est difficile de trouver de tels sources sur Internet car n'importe quel utilisateur Lambda pourra lancer sur son propre PC ou bien encore l'envoyer a ses « amis ».

La seconde solution c'est porté sur notre compte Gmail. Il n'est pas rare de recevoir de nos meilleurs fournisseurs des spams contenant des petits programmes malsain. Mais nous avons remarqué que « MR Gmail » les supprimaient et n'afficher que le message.

Enfin, la dernière solution a été de mettre en place une machine directement sur internet et aller sur des sites permettant d'installer des ActivesX douteux ou bien encore télécharger par notre logiciel de torrents les petits fichiers de quelques KO. Afin de récupérer le fameux virus.
Au final nous avons récupéré beaucoup de virus mais pas conficker.C.

Notre outil de supervision nous indiquait bien une montée en charge du réseau ainsi que l'augmentation des processus des machines. Mais rien de significatif et qui ressemblait à Conflicker.c.

2. Clavier Keylogger

a. Contexte

L'entreprise possède un nombre très important d'équipements au sein de ses bâtiments, et parfois à l'extérieur chez des clients, sous-traitants, hébergeurs, réparateurs… Bien souvent la sécurisation physique de ces équipements n'est pas réalisée de manière complète, car on considère qu'en dehors des serveurs jugés « cruciaux », les autres machines ne représentent pas un réel danger.

Dans la réalité, et nous avons pu le démontrer lors de ce projet, **la compromission d'un accès physique permet de récupérer énormément d'informations**. Par ailleurs, **aucune détection logicielle** n'est possible, et donc sans réelle politique de sécurité à ce niveau, l'entreprise peut en être victime pendant des années sans jamais le soupçonner ni le détecter.
Ce type d'attaque matériel doit pouvoir être reproduit à des niveaux différents : dupliquer interface SATA des disques dur, dupliquer l'affichage, clavier sans fil, caméra d'enregistrement.

b. Preuve de concept sur les keylogger matériels

Lors de nos recherches, nous avons pu trouver un fournisseur qui a conçu des **keylogger matériels** avec les propriétés suivantes :

- compatible avec les claviers PS2 et USB de manière transparente (identifiant USB, pas de retard) ;
- invisible pour un modèle localisé à l'intérieur du clavier ;
- capacité mémoire de 4Mo à 16Go ;
- très simple à monter et à exploiter ensuite ;
- avec la possibilité d'y greffer un module sans fil pour accéder aux enregistrements.

L'entreprise fournit aussi les spécifications d'un keylogger matériel « open-source », avec la liste des éléments électroniques qui le composent, le schéma électronique ainsi que le code assembleur pour le microcontrôleur.

c. *Description du montage*

Voici comment transformer un clavier d'apparence normal, en un clavier « intelligent ».

Le montage nécessite juste de réaliser 2x4 soudures pour intercaler la carte entre le clavier et le PC. Les keylogger de ce fournisseur sont très aboutis, puisqu'ils prennent en compte les layouts des différents pays, enregistrent les touches spéciales etc…

Pour accéder aux données :

- clavier PS2 :
  - Combinaison à 3 touches permettant d'accéder au menu d'administration, et rejouer les logs ;
  - Montage en USB mass storage à l'aide du cable adéquat.
- Clavier USB :
  - Combinaison à 3 touches permettant de monter la mémoire en USB mass storage, et copie du fichier.

Les avantages pour un « attaquant » de ce type de solution :

- Peu onéreux ;
- Indépendant du système d'exploitation ;
- Réutilisable ;
- Invisible ;

Conclusion :

Le keylogger fait partie des classique de l'attaque informatique, et la plupart des virus et rootkit en intègre un. Une fois en place, il permet de récolter une somme très importante de données qui ne seraient pas forcément accessibles sans.

- Indétectable ;
- Possibilité de faire évoluer la version open-source ;
- Accès sans fil pour accéder aux données.

d. Nos actions

Nous avons donc modifié 5 claviers de cette manière :

- 4 claviers Cherry PS2, utilisés sur les postes clients et les serveurs d'applicatifs de CandideSA ;
- 1 clavier Dell USB, utilisé sur le routeur FreeBSD de CandideSA.

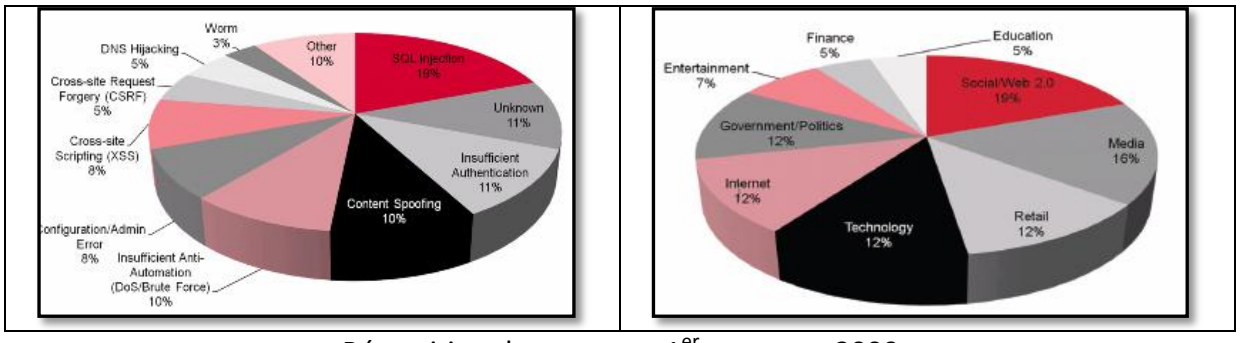
Régulièrement, nous sommes passé dans la salle, comme aurait pu le faire un intervenant externe à la société pour décharger les informations des claviers et voir ce qui était potentiellement exploitable.

3. WEB 2.0

a. Contexte

Les applications collaboratives ou réseaux sociaux orientées 2.0 sont souvent d'excellents moyens de diffusion ou mines d'information pour les hackers.

« The web hacking incident database » est un projet visant à maintenir une liste des incidents de sécurité liés aux applications web. D'après le rapport bi annuel émis par Breach Security Labs (août 2009), les cibles des 44 incidents reportés au premier semestre 2009 se répartissent comme suit :



Répartition des attaque, 1er semestre 2009.

D'après ce rapport, les attaques de sites 2.0 et notamment des sites de type « réseau social » (twitter, facebook…) sont en constante augmentation. De même, les « injections SQL » diminuent au profil des attaques de type « Cross-Site Scripting » ou « Cross-site request forgery », plus adaptées au web 2.0.

Dans le cadre du projet de sécurité M2 STRI, ce constat nous a amené à nous **focaliser sur l'audit de l'application web 2.0 déployée par l'équipe défense : Wordpress 2.8.6.** Pour cela, nous avons commencé par nous renseigner sur **les types d'attaques** à la mode, puis sur les outils d'audit existants avant d'effectuer des tests sur la plateforme Wordpress. Ces résultats nous ont permis d'émettre un certain nombre de **recommandations visant à augmenter la sécurité** de cette application.

b. Audit de Wordpress

Les tests d'audit qui suivent ont été réalisés sur un serveur personnel (sous debian squeeze) sur lequel avait été déployé Wordpress (deux articles, deux commentaires dont un invalidé). Cette configuration ne représente certes pas la situation de Candide SA, qui dispose de toute une équipe dédiée à la sécurisation de son infrastructure informatique. Ici la configuration des paquets est celle fournie par défaut lors de leur installation. Cette situation peut représenter celle d'une petite entreprise qui sous-traite la gestion de son parc à une autre société.

La source est une machine virtuelle présente sur le réseau local et utilisant l'OS Samurai (v0.7). Cette distribution basée sur Ubuntu implémente de nombreux outils d'audit et d'attaque de plateformes web. Son objectif est de devenir la distribution de référence dans ce domaine (devant Backtrack).

DirBuster

DirBuster est une application qui permet de « bruteforcer » les dossiers contenus dans une application web. DirBuster va tenter de faire correspondre des répertoires présents sur le serveur avec une liste de répertoires. Le but de cette application est donc de découvrir l'arborescence du serveur web et de trouver des dossiers / fichiers sans liens pointant vers eux.

L'éxécution de DirBuster à la racine du serveur web (avec comme entrée le dictionnaire « big » fournit sur Samurai) permet de récupérer l'arborescence des dossiers et fichiers du Wordpress.

ZeNmap

ZeNmap est une interface graphique de l'outil Nmap. Nmap est un excellent outil utilisable uniquement en ligne de commande. Les fonctionnalités proposées par ZeNmap vont du simple scan aux scans très précis en passant par la détection de systèmes d'exploitation distants.
ZeNmap en plus des services proposés par la machine, nous à donné la version d'apache et du système d'exploitation :

<service product="Apache httpd" name="http" extrainfo="(Debian) PHP/5.2.6-1+lenny4 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_perl/2.0.4 Perl/v5.10.0" version="2.2.9" conf="10" method="probed">

Recommandations pour la sécurité :

L'ajout de fichiers .htacces dans les répertoires permettra de limiter les effets de DirBuster.

W3AF

W3AF (**Web Application Attack and Audit Framework**) est un logiciel entièrement écrit en Python. W3AF est un Framework très complet orienté vers les audits et les attaques à l'encontre des applications web. Il est divisé en deux parties :

- Le core qui gère les processus et la communication entre les plugins ;
- Les plugins étant classés en 7 catégories distinctes (découverte, audit, grep, attaques, affichage, modifieurs de requêtes, évasion et brute force).

Le Framework dispose d'une interface graphique très complète et très intuitive pour l'ensemble des actions qu'il propose. Le projet contient de nombreux plugins qui permettent de chercher pour les injections SQL, les injections XSS, les inclusions de fichiers locaux/distants et bien plus encore.

Le profil choisi pour ce test est le « Full Audit », qui intègre les plugins d'audit, brute force, découverte et grep.

Résultats :

The URL: http://192.168.0.2/wordpress/template.php is vulnerable to cross site request forgery.

Il s'agit d'une faille recensée dans les versions de Wordpress indérieures à 2.8.5. Elle concerne le champ de formulaire « url » qui permet à l'auteur d'un commentaire de donner l'adresse de son site. Par exemple, si on entre le code suivant :

http://www.nioutaik.fr'onmousemove='javascript:alert()

l'html résultant sera :

<a href='http://www.nioutaik.fr'onmousemove='javascript:alert();' rel='external nofollow' class='url'>

Ainsi au moment ou l'utilisateur passe sa souris sur le lien, le code JavaScript est exécuté. Ce code pourrait déclencher une redirection vers un autre site imitant l'interface de login de wordpress. Un administrateur non avertit pourrait ainsi fournir son login / mot de passe.

Recommandations pour la sécurité :

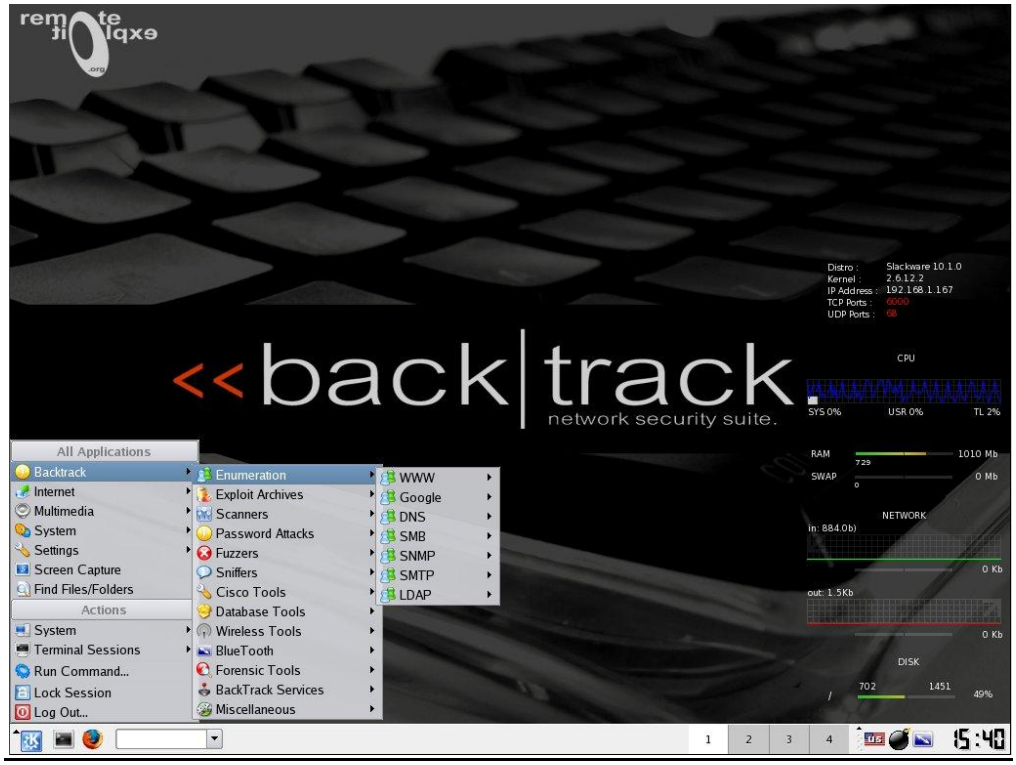
Une configuration plus attentive du service apache est nécessaire (ServerTokens Prod, ServerSignature Off). La sécurisation d'apache passe par la désactivation des modules inutiles et l'installation et la configuration des modules de sécurité (mod-Security, mod-evasive…). Une bonne configuration d'apache permettra de se protéger contre de nombreuses attaques, par exemple contre le fameux script PHP de 36 lignes utilisé par l'équipe attaque pour faire tomber le serveur hébergeant le Wordpress (http://rooibo.wordpress.com/).

c. *Le Live CD BACKTRACK*

Présentation de BackTrack

Backtrack est un live cd basé sur la distribution SlackWare. Cette distribution est le résultat de la combinaison entre Whax et Auditor. Son objectif est de fournir un ensemble d'outils permettant l'analyse réseau et des outils permettant de tester la sécurité. La dernière version stable est la version 3.0 depuis le 19 juin 2008, une Pre- Release 4 est en cours de test. Ce nouveau release est maintenant basésur Debian.
Backtrack emporte plus de 300 logiciels permettant de découvrir des topologies, scanner des ports, craquer des réseaux wifi ou des mots de passe ou encore exploiter les données SNMP.
Ce live CD contient des outils permettant de scanner et de sortir des configurations de routeur Cisco, de faire des attaques sur des bases SQL, de tester les paramètres Samba, des outils d'injection SNMP et beaucoup d'autre encore.

Voici une image de Backtrack :



Les avantages et les inconvénients de BackTrack

Les live CD sont des distributions directement installé sur un cd et bootable directement sans installation sur le disque dur. Elles permettent de tester et éventuellement installer par la suite ces distributions. Ces live CD sont souvent exploitable via Clé USB ce qui les rend encore plus puissante puisque l'enregistrement et l'installation de nouveau logiciel est possible.
Néanmoins, étant sur un support amovible, la configuration ainsi que les matériels prient en charge sont limités, le démarrage peut être long si la distribution est chargé dans la RAM.

Avantages	Inconvénients
Pas de modification de la machine	Lenteur
Distribution prête a l'emploi	Pas de sauvegarde de données si support CD
Permet de tester le support des matériels	

Nous avons utilisé quelques live CD pendant le projet sécurité :

- RemoteExploit Back|Track
- CentOS
- OSSIM

Ces live CD nous ont permis de monitorer ou de tester l'infrastructure de la défense.

VI. Bilan technique

Après chaque confrontation, plusieurs comptes rendus d'audit ont été rédigés pour la société Candide SA. Ils avaient pour but de décrire et commenter les actions menées par l'équipe d'attaque afin d'infiltrer et éventuellement de corrompre le système d'information de la défense. Notre rôle a été d'analyser les flux de donnée transitant entre l'équipe attaquant et l'équipe défense.

1. Les différentes confrontations

a. Confrontation 1

- **Les outils**

L'équipe défense nous fournit les logs système de leurs serveurs. Grace à NetFlow, nous traitons le fichier, Netflow analyse les flux entrant et nous remonte automatiquement les alertes ce qui nous permet d'aisément analyser le trafic.

Des sondes Snort ont aussi été placées afin de visualiser le type et la quantité de trafic qui circule.

- **Observations durant la confrontation**

Au départ, l'attaque a lancé un port scan. Elle lance des scans via Nmap pour découvrir la topologie du réseau de la défense, la défense voit passer les scans et bloque les IPs scannant le réseau. Par la suite, l'équipe attaque décide donc de faire un scan de port.

Ensuite le groupe a fait du Webroot Traversal : Le Webroot traversal est un type attaque qui a pour principe de rentrer sur le répertoire du serveur web. Par la suite il sera possible d'exécuter des commandes afin de s'introduire sur la machine hackée.
Ce type d'attaque a échoué.

L'équipe attaque a tenté de s'introduire sur le blog de Candide SA afin d'exécuter du code JavaScript sur « login.php ».

- **Constatation**

L'attaque n'a pas été virulente et ses attaques ont été arrêtées. L'équipe défense a réagi en temps réel ce qui n'a pas permis à l'attaque de s'introduire dans l'infrastructure. En effet les IPs suspectent étaient directement bloquées. La confrontation n'a donc démontré que les services mis en place par la défense étaient sur.

b. Confrontation 2

- **Observations durant la confrontation**

Snort via la console Acid, nous permet de remarquer une attaque plus ciblée sur la machine 10.200.0.8 via le service HTTP sur le port 80 depuis l'adresse 172.16.0.2 (Casper) et le port 41321. Cette adresse nous indique que c'est une machine située dans le réseau interne, qui passe à travers Casper.
Le type d'attaque est réalisée par des requêtes de type WEBROOT DIRECTORY TRAVERSAL, afin de découvrir les différentes pages délivrées par le serveur Web, et le type de contenu (statique, dynamique).

Le but supposé de ce scan intensif est de générer un bruit de fond, et un stress constant sur le service HTTP. En parallèle, l'attaque a lancé une attaque sur une faille connue du script Wordpress (publiée le 17/10/2009, par son auteur à l'adresse http://rooibo.wordpress.com/).

Suite à cette attaque, le serveur hébergeant le service HTTP est injoignable, le déni de service a fonctionné.

- **Constatation**

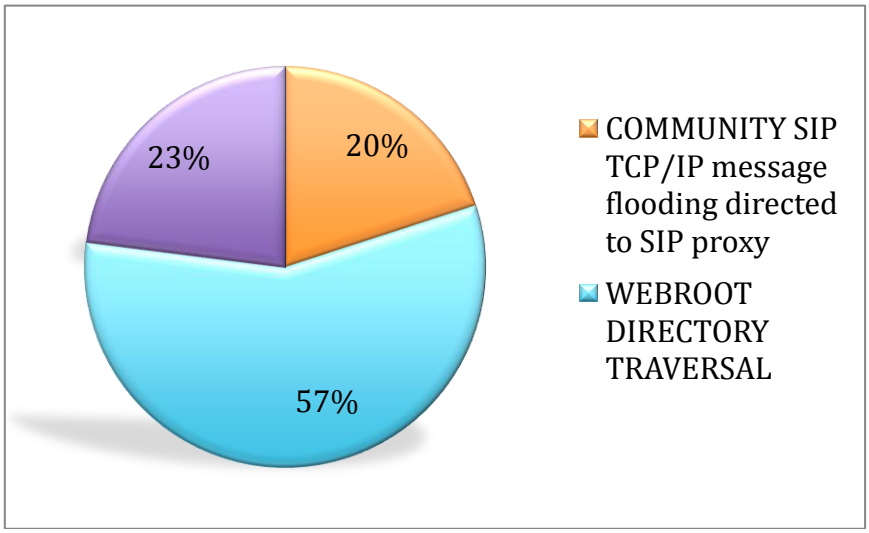
L'équipe attaque a réussi à exploiter une faille de sécurité dans Wordpress, l'exploit est fonctionnel puisque les services et le serveur n'ont pas pu être exploités pendant une période relativement longue.

L'équipe attaque a pu uploader un document PDF vérolé par Trojan.Pidief.G.
L'entreprise Candide S.A a su réagir rapidement car l'indisponibilité du serveur et des services FTP et HTTP n'a pas dépasse les 40 minutes.

- **Conclusion**

Les faiblesses ainsi que nos conseils au groupe défense se trouvent dans le second rapport traitant de l'ensemble des préconisations ainsi que des faiblesses des choix faits par la défense.

Voici un diagramme montrant la repartions des attaques majeures:



c. *Confrontation 3*

Cette confrontation a commencé que tardivement. La stratégie du groupe défense était que seul le chef de projet technique détenait les mots de passe des machines. Etant en retard, la confrontation a donc commencé avec 1h30 en retard, ne laissant pas beaucoup de temps à l'attaque de simuler des intrusions vu le créneau prévu pour la séance.

Une attaque du réseau WIFI a été réalisée. En effet l'équipe attaque a réussi à pirater la borne Wifi ce qui aurait pu être évité si l'équipe défense avait accepté une confrontation avec l'équipe « analyste ». Nous aurions pu proposer de meilleures solutions de chiffrement et d'installation.
(Pour les préconisations cf. rapport 2)

2. Les résultats de l'intrusion à l'aide des claviers Keylogger

Les claviers espions nous ont permis de déterminer de récupérer des informaton du groupe défense.

Les premières informations intéressantes sont apparues rapidement :

- Passphrase de chiffrement des disques dur ;
- Mot de passe root des serveurs et du routeur FreeBSD ;
- Identifiant du wiki d'un utilisateur, pour lequel il manquait le code à 3 chiffres saisi à la souris ;
- Différents identifiants de webmail et autres sites de nombreux utilisateurs.

A titre informatif, nous allons publier la liste non exhaustive des informations enregistrées :

Service	Fournisseur	Victime	Rebond possible
Mail	hotmail	adilnoua	OUI
Mail	gmail	adilnoua	OUI
Mail	hotmail	alex_clamart	OUI
Mail	hotmail	ladyrama2006	OUI
Mail	gmail	lisebanquet	OUI
Mail	gmail	cyrille.dumas	OUI
Mail	orange	vduvivier	OUI

L'entreprise CandideSA n'a pas envisagé la sécurisation physique de son parc de machines.
En conséquence, ce type d'attaque a été facile à mettre en œuvre. Comme nous l'avons déjà dit dans des précédents rapports, les utilisateurs n'ont pas été sensibilisés sur les problèmes d'utilisation de machine non contrôlé par l'entreprise. (Les machines dont l'accès n'est pas vérifié ou vérifiable)
Le matériel a pu rester en place pendant 3 semaines, et même après la fuite de données simulée les comportements n'ont pas évolué, puisque les mots de passe ont pu être enregistrés par nos claviers.

VII. Conclusion

A travers ce projet, nous avons ou découvrit le métier de l'analyste. Le travail consiste en plusieurs étapes nécessitant une veille technologique importante ainsi qu'une préparation d'un plan d'action. L'analyse doit être structurée 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.
Nous avons pu découvrir un ensemble d'outils et de méthodes pour surveiller un réseau d'entreprise ainsi que les dangers des attaques dans des réseaux d'entreprise.

Le projet a été une expérience enrichissante. Il a permis d'aborder une vision réelle de projets longs qui seront amenés à se réaliser en entreprise. Il nous a permis d'apprendre à gérer l'organisation d'une équipe, à mettre en place une gestion du temps et des contraintes, de prendre conscience de la place prépondérante de l'aspect relationnel au sein d'une équipe ainsi qu'avec le client. L'aspect relationnel avec l'équipe défense nous a confortés dans l'idée que la communication peut être un point délicat

Enfin, cette expérience sera très utile pour affronter le monde du travail tant d'un point de vue technique que relationnel.

ANNEXES

Annexe 1 : Réunion de précontrat entre la Défense et l'Audit

Informations sur le réseau		
Ce que nous souhaitons connaître:	Oui	Non
- un organigramme du personnel + rôles	X	
Commentaire :		
- la charte d'utilisation des ressources	X	
Commentaire :		
- l'architecture réseau (topologie, plan d'adressage architecture réseau, os systèmes)	X	
Commentaire :		
- le matériel utilisé (modems, routeurs, commutateurs, pare-feux)		
Commentaire :		
- Connaitre la gestion des droits sur les postes de travail, les serveurs ainsi que les services qu'ils délivrent, les applications, les solutions antivirales, version d'apache du site web.	X	
Commentaire :		
- journalisation des logs, informations SNMP.	X	
Commentaire :		

Périmètre d'actions		
Les actions que nous pouvons mener :	Oui	Non
- Organiser et planifier des interventions et ses entretiens avec les personnes à interviewer au sein de la défense	X	
Commentaire : *A ajouter une partie confidentialité*		
- Faire des rapports pour des recommandations, pour la mise en	X	

place de mesures organisationnelles et techniques ??		
Commentaire : Toutes les semaines (mêmes si rien a préciser)		
- Avoir un accès physique au système pour la mise en place d'outils d'analyse et de détection (analyse des logs, scans, sondes)	X	
Commentaire : Rediriger Tous les logs sur notre vlan		
- Effectuer des tests d'intrusions ? Avec rapport	X	
Commentaire : Planification + rapport		
- Gestion de la supervision	X	
Commentaire : Installation+ vlan specifique		
- Possibilités de modification sur Routeur+ Switch	X	
Commentaire :		

Compte-rendu :		
Les rapports peuvent traiter :	Oui	Non
- rapport complet a chaque phase d'analyse	X	
Commentaire :		
- proposer des améliorations techniques et organisationnelles	X	
Commentaire :		
- La défense doit prévenir l'audit de tout changement.	X	
Commentaire :		

Modification de Contrat :		
Termes du contrat	Oui	Non
- modifications de contrat des Avenants seront produits et devront être obligatoirement signés par les deux partis que ce soit pour une modification mineure ou majeure afin que tout compromis soit évité ??	X	

Commentaire :		
- Pour chaque question posée à la défense, l'audit attendra une réponse rédigée sous 48h (pour une meilleure réactivité de l'équipe audit).	X	
Commentaire :		
- Toutes modifications sur les systèmes et les équipements ne pourront être réalisé 72h avant la date des différentes confrontations.	X	
Commentaire :		

Points à définir :		
Echanges des données	Oui	Non
- pour l'échange de données (moyen de communication) nous vous proposons d'échanger les données avec le système de clé public et clé privé. Si oui alors c'est très bien sinon que proposez-vous ?	X	
Commentaire : Par le biais de clef public et privée définis, mais un seul interlocuteur. Ou système de la défense.		
- Accès à distance	X	
Commentaire :		

Annexe 2 : Contrat de prestation de service

Article 1 – Divulgation des informations entre les 2 entités
La société Candide SA s'engage à fournir les informations concernant :

- L'organisation de son personnel, ainsi que les noms, coordonnées des interlocuteurs spécifiques et leur rôle au sein de cette dernière.

- L'architecture de la solution réseau qu'elle déploie (topologie, adressage, les règles de filtrages).
- Les types de systèmes d'exploitation utilisés pour les postes clients, les serveurs et les équipements d'interconnexion.
- La charte d'utilisation des ressources du personnel.

Article 2 – Définition du périmètre d'action de l'audit

Ayant connaissance des éléments composant le Système d'Information :

- L'auditeur pourra organiser et planifier ses interventions et ses entretiens avec les personnes à interroger au sein de la société.
- L'équipe d'analyse sera responsable de l'organisation des réunions avec l'équipe auditée et devra, à l'issue de celles-ci, proposer des recommandations pour la mise en place de mesures organisationnelles et techniques.
- La société devra mettre à disposition des moyens permettant à l'auditeur d'assurer sa mission d'ingénierie d'analyse et de conseil (mise en place de canaux de communication dédiés, vue sur l'ensemble des "logs" système et réseaux).
  Typiquement via l'utilisation de syslogd, de commutateurs configurés avec Port Mirroring, par la configuration de communautés SNMP ou encore d'un collecteur netflow mis en place sur un serveur suite à la topologie matérielle choisie .
- L'auditeur pourra planifier conjointement avec la société Candide SA des tests d'intrusion effectués selon des scénarios d'attaque, afin de déterminer les vulnérabilités et failles de sécurité.
- L'auditeur bénéficiera de ressources systèmes dédiées, qu'il pourra installer dans les locaux de la société, et sur lesquelles il pourra intervenir et mettre en place des solutions d'analyse, supervision et de détection.
- L'auditeur disposera d'un rôle de conseil et pourra donc faire des demandes motivées de modifications auprès de la société.

Article 3 – Communication et Résultats

- Chaque phase d'analyse et d'évaluation réalisée par les soins de l'auditeur devra donner lieu à la réalisation d'un rapport complet présentant de manière explicite les vulnérabilités détectées sur le système audité et proposant des améliorations techniques et organisationnelles pouvant entraîner une revue de la politique de sécurité.
- A son tour la société Candide SA devra informer l'auditeur de toute modification ou évolution de la topologie du système de sécurité.
- Un rapport hebdomadaire, permettant de constater l'activité du réseau, sera remis à la société Candide SA.
- Pour chaque question posée à la société Candide SA, l'auditeur exigera une réponse rédigée sous 48h.
- Les données et rapport devront être échangés via le système de communication sécurisé prévu à cet effet, à l'initiative de l'auditeur ou de la société Candide SA.

Article 4 – Modification du Contrat

- Dans le cas de modifications du contrat, des Avenants seront produits et devront être obligatoirement signés par les deux parties.

Article 6 – Accès distant à l'infrastructure

- La société Candide SA s'engage à fournir un accès sécurisé de type VPN accessible en dehors des locaux. Cet accès permettra à l'équipe analyse d'accéder à l'ensemble des équipements qu'elle aura pu installer au sein de l'entreprise Candide SA.

Article 7 – Confidentialité

- L'auditeur, à savoir l'ensemble des personnes qui interviendront pour la mission d'audit de sécurité, s'engage, sous sa responsabilité exclusive, à considérer confidentielles toutes informations transmises par la société Candide SA, de façon orale ou écrite, et par conséquent à ne pas les divulguer à un tiers. Une clause de confidentialité sera établie à l'initiative de la société Candide SA et devra faire l'objet d'une signature par l'ensemble des membres composant la société d'audit.
- La société d'audit assume l'entière responsabilité de la sécurisation des équipements et sondes, et des accès au réseau de la société Candide SA qu'ils peuvent occasionner.
- De la même manière, les différents droits octroyés à l'organisme d'audit sont placés sous leur entière responsabilité.
- Les sanctions prévues dans ce contexte d'activité sont la simple reconnaissance écrite des fautes dans le cas où une responsabilité est engagée.

A Toulouse, le ……

Signature, précédée de la mention "Lu et Approuvé"