Master 2

STRI
| Télécoms & Réseaux |

Projet de Sécurité

Groupe Analyse

Réalisé par :

Arnaud Sébastien
Bizouard Paul
Delomier Yoann
Esquié Jérôme
Falguera Anne
Laudic Sébastien
Salvan Lydie

Présentation du sujet

- Maquette d'infrastructure d'entreprise
- 3 groupes de travail :
  - Groupe Défense
  - Groupe Attaque
  - Groupe Analyse

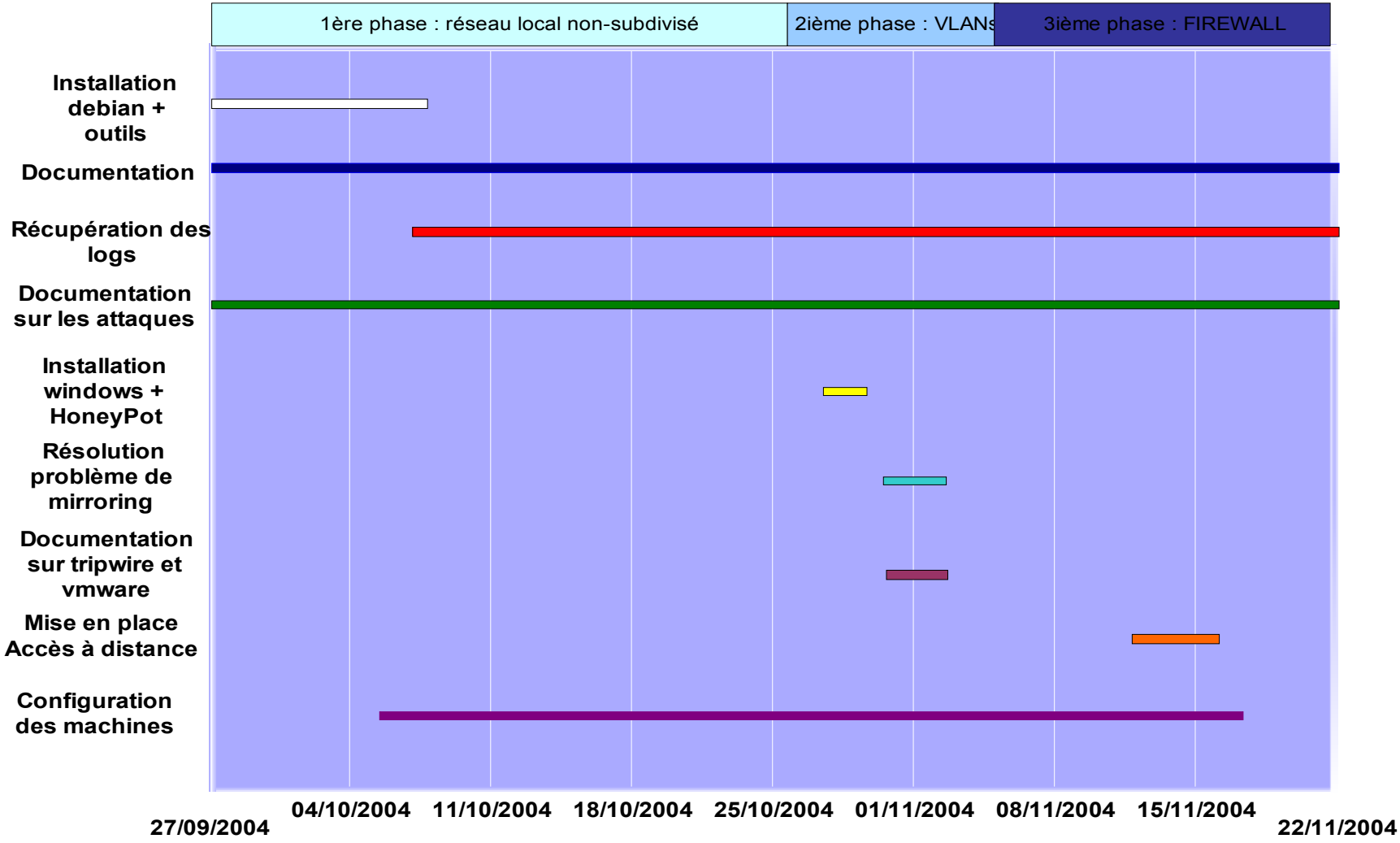
Objectifs

- Travail en équipe
- Difficultés de la sécurité informatique
- Métiers concernant l'audit d'un réseau informatique
- Communication entre les groupes ayant des rôles et des objectifs différents

But des analystes

- Récupérer les fichiers log
- Repérer les attaques qui ont réussi et celles qui ont échoué grâce aux précautions prises par l'équipe Défense

Présentation des phases



Plan

- Les outils utilisés
- Par phase :
  - Les changements d'architecture
  - L'évolution de la méthode d'analyse des logs
  - Un bilan
- Bilan du projet

Les outils utilisés

Ethereal (1/3)

Caractéristiques

- Outil gratuit sous licence GNU
- Récupère les paquets et les interprète
- Capture ou lit un fichier de capture
- Graphique ou ligne de commande (tethereal)
- Plus de 602 protocoles
- Deux sortes de filtres

Ethereal (2/3)

Filtres de capture

- Ne seront gardés que les paquets pour lesquels le filtre est vrai
- Décomposition en trois parties
  - protocole (**ether**, **fddi**, **ip**, **arp**, **rarp**, **tcp** ou **udp)**
  - direction (**src** ou **dst**)
  - champ (**host**, **net** ou **port** suivi d'une valeur)
- Utilisation d'opérateurs (and, or, not) pour combiner des filtres

Ethereal (3/3)

Filtres d'affichage

- Plus fins que pour les filtres de capture
- Expression du filtre basée sur les champs disponibles dans un paquet
- Utilisation d'opérateurs (**==**, **!=**, **>**, **<**, **>=** et **<=**) pour comparer les champs à des valeurs précises
- Combinaison de filtres à l'aide d'opérateurs (&&, ||, ^^, !)
- **Exemples de champs disponibles :**

champ	champ
ip.addr	icmp.code
ip.dst	icmp.type
ip.flags.df	ftp.request
ip.flags.mf	ftp.request.command
ip.ttl	ftp.response.data
nbdgm.src.ip	dns.query
nbdgm.src.port	dns.response
http.request	

SNORT (1/4)

- Système de détection d'intrusion réseau (NIDS)
  - Mode sniffeur
  - Mode enregistreur de paquets
  - Mode détection d’intrusion
- Analyse du trafic en temps réel et journalisation
- Portable sur plusieurs types de plateformes
- Installation et configuration simples
- Écriture des règles
- Logiciel libre de droit

SNORT (2/4)

- **Détection au niveau des protocoles** :
  -IP -TCP -UDP –ICMP …

- **Détection d'activités anormales**
  - Stealth scan
  - Découverte d'empreinte d'OS
  - Code ICMP « invalide »

- **Détection de dénis de service**

- **Détection de débordement de buffer**

SNORT (3/4)

Avantages

- Installation simple et rapide
- Nombre de règles conséquent
- N'engendre pas de ralentissement du trafic
- Logiciel libre
- Simplicité d'écriture des règles

SNORT (4/4)

Inconvénients

- Ne détecte pas tout
- Pas d'interface graphique
- Gestion des rapports difficile avec la prolifération des sondes
- Une veille technologique est obligatoire pour la mise à jour des règles
- Certifié pour les réseaux 10 Mbits

SNORTSNARF

- Programme PERL
- Génère des pages HTML à partir des fichiers d'alertes SNORT
- Simplicité d'installation et de mise en place
- Une petite démonstration...

HoneyPot : Back Officer (1/2)

Principe du pot de miel

- Attirer l'attaquant
- Simuler une machine vulnérable
- Trace des attaques pour :
  - Identifier l'attaquant
  - Déterminer les attaques menées

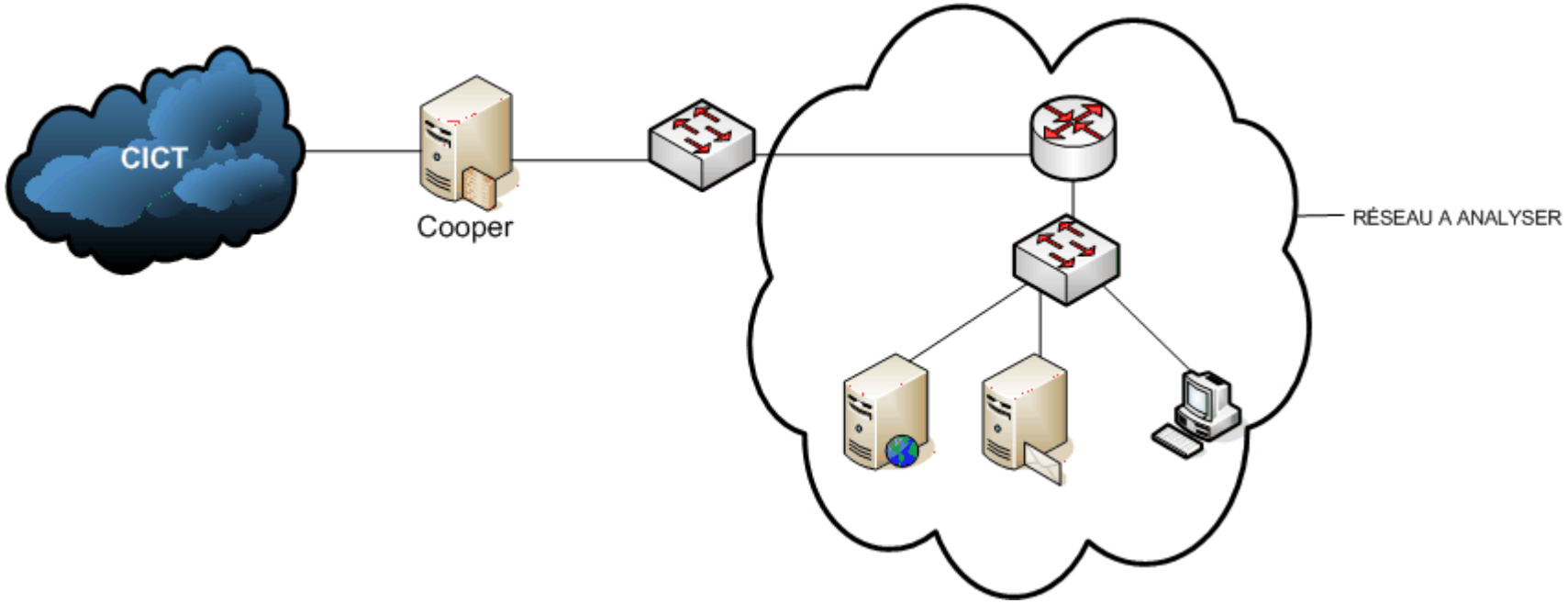
HoneyPot : Back Officer (2/2)

- Pourquoi Back Officer?
  → Simple et gratuit

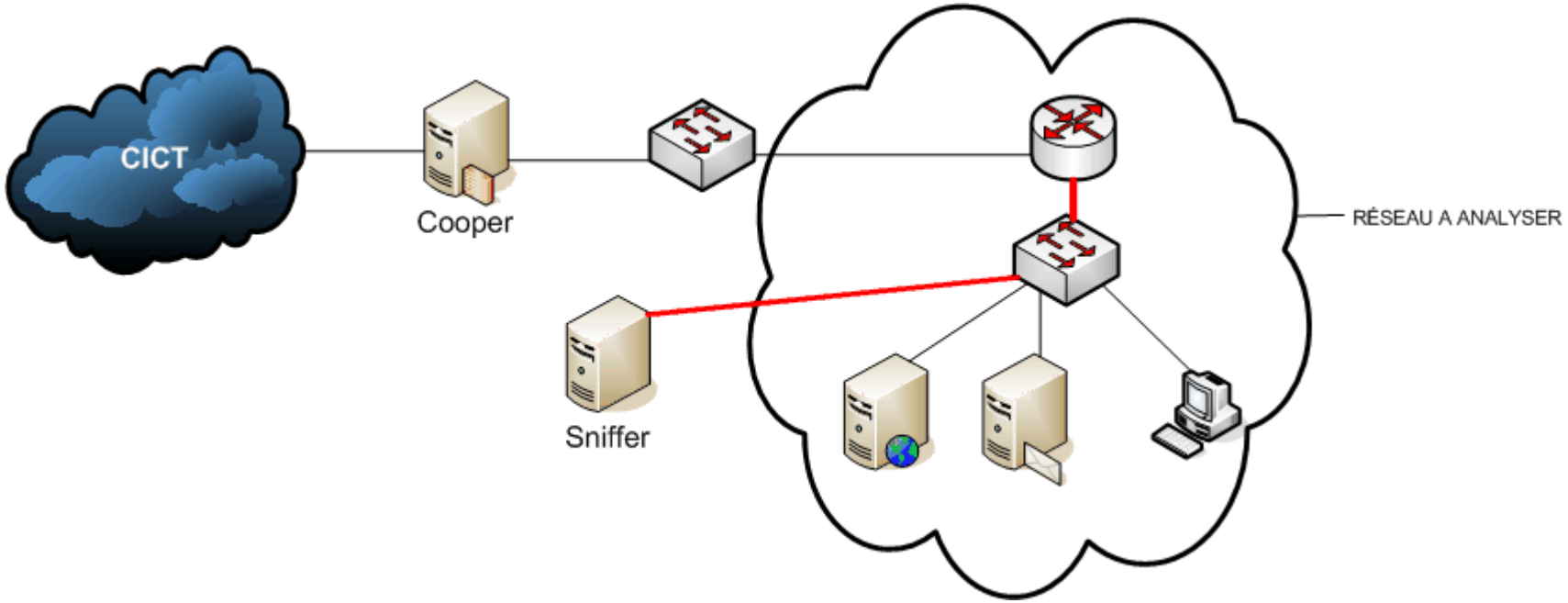
- Fonctionnement
  → Emule les ports les plus courant

Phase 1

Architecture (1/2)



Architecture (2/2)



Méthode d'analyse (1/3)

Entraînement sur un scan du projet Honeynet

Premier log de 1Go à cause du générateur de bruit

- Nécessité de mettre rapidement en place l'accès distant
- Méthode d'analyse à revoir

Méthode retenue

- Génération des alertes Snort
- Organisation de ces alertes pour lister les attaques par machine
- Section des logs par machine pour observer ces attaques dans Ethereal
- Analyse de la réussite des attaques
- Calcul des statistiques des attaques
- Rédaction du rapport

Méthode d'analyse (2/3)

Présentation d'une attaque:

- Cible : le serveur Web(172.66.66.5)
- Date : 14 octobre 2004

Alertes Snort

```
[**] [1:249:8] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
10/14-21:11:06.233524 172.16.80.250:58560 -> 172.66.66.5:15104
TCP TTL:62 TOS:0x0 ID:38750 IpLen:20 DgmLen:60 DF
******S* Seq: 0x8E27310D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 33793619 0 NOP WS: 0
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138]
```

SID de l'alerte

Nom de l'alerte

Classification de l'alerte

Priorité l'alerte

Date

Adresses et ports destination et source

Infos TCP

Lien concernant l'attaque

Méthode d'analyse (3/3)

Section du fichier log à partir de la date pour l'analyser avec Ethereal

Analyse de l'attaque dans Ethereal : 
Ethereal.exe

Bilan de l'analyse des attaques durant la phase1

- Longue et fastidieuse
- Méthodologie de départ totalement repensée
- Meilleure connaissance des flux sur le réseau
- Meilleure connaissance des attaquants
- Nécessité de repérer les faux positifs

Bilan pour la phase 1

Définition d'un faux positif

Message légitime considéré à tort comme une attaque, ce qui entraîne l'émission d'une alerte.

Caractéristiques

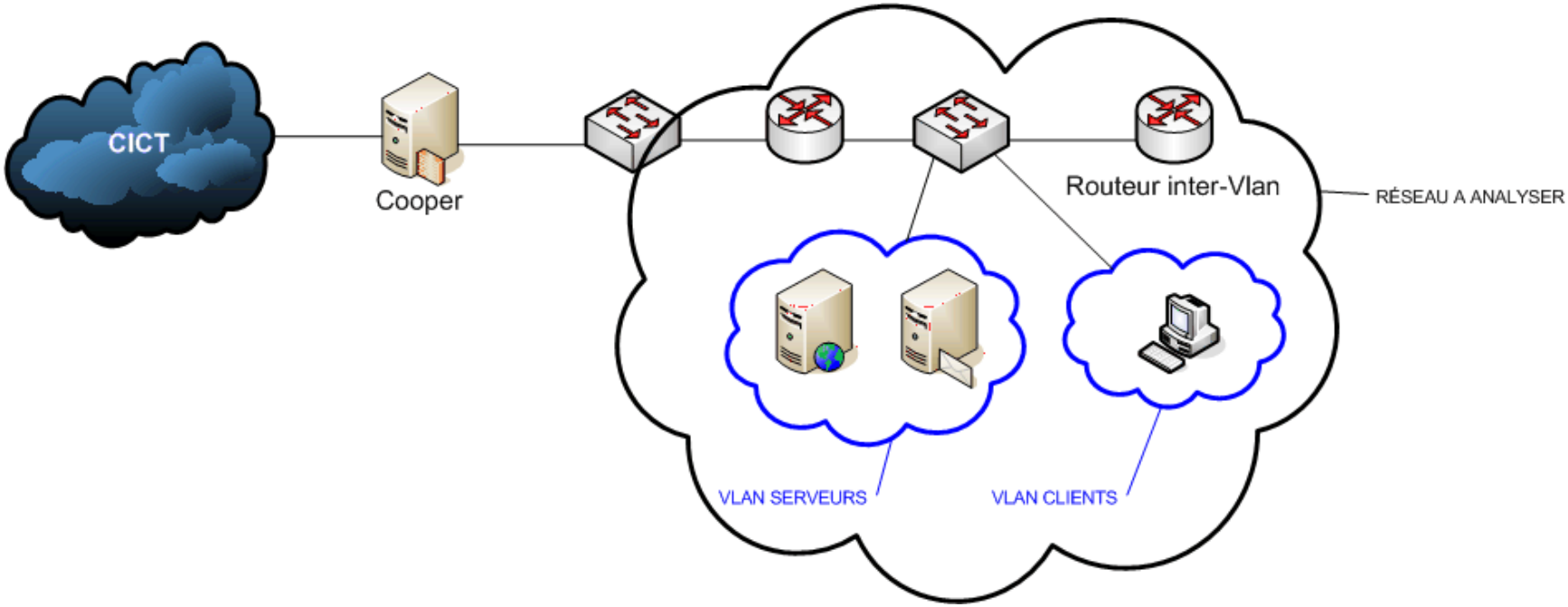
- Emises par des machines n'appartenant pas à l'équipe attaque
- Quantité importante dans nos logs

Conséquences

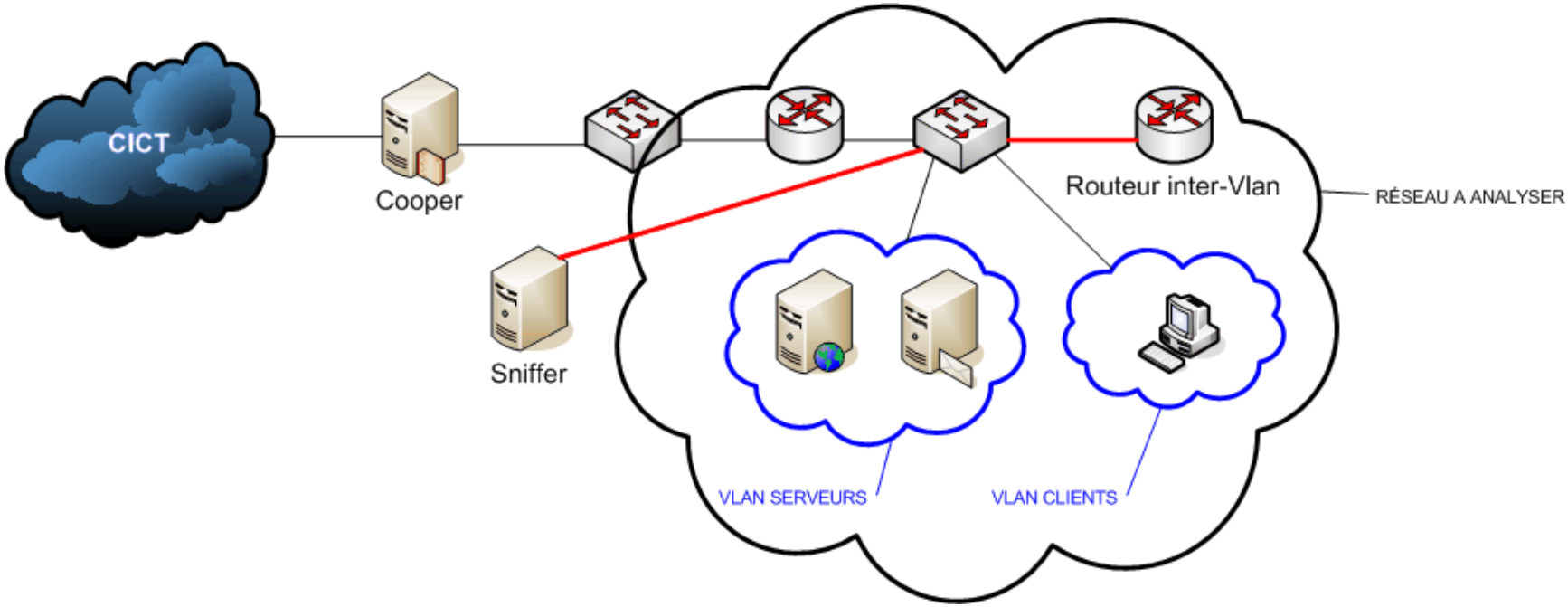
- Augmentation de la taille des fichiers de logs
- Augmentation du temps d'analyse (et donc perte de temps)

Phase 2 : Mise en place de VLANs

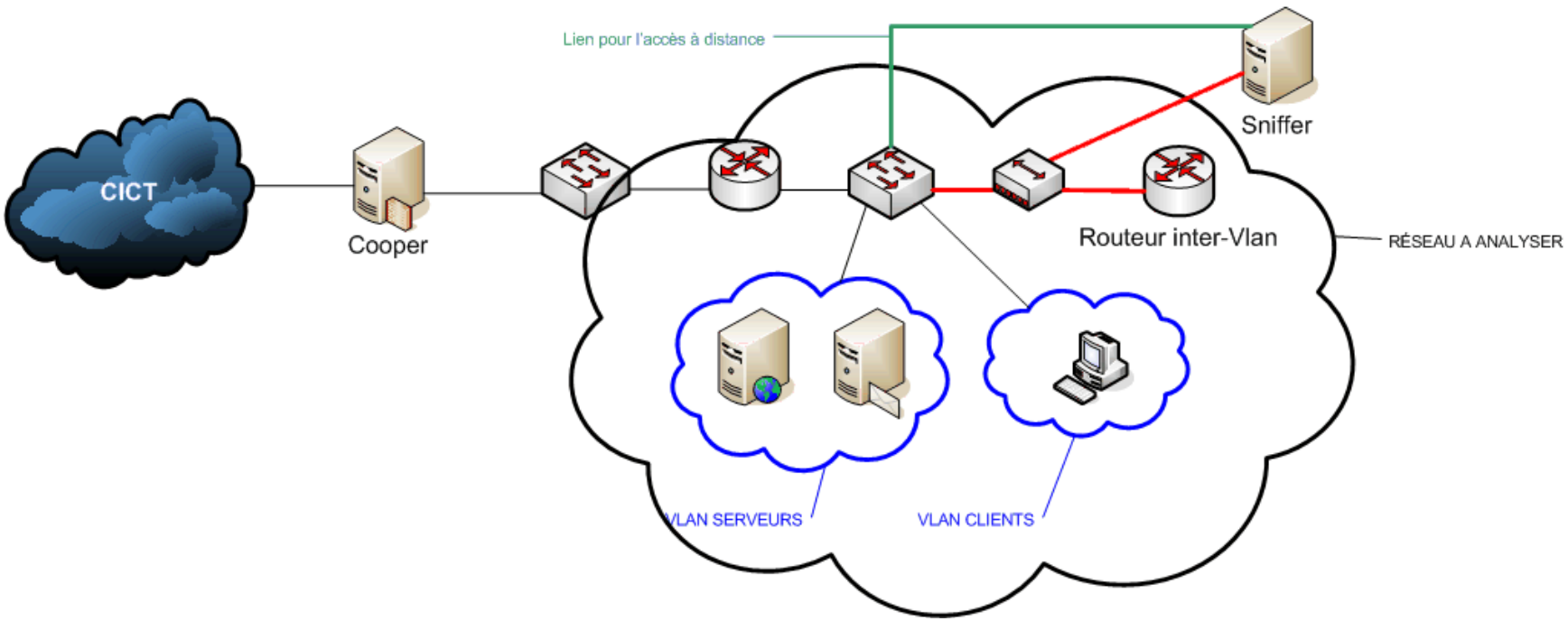
Architecture (1/3)



Architecture (2/3)



Architecture (3/3)



Méthode d'analyse (1/3)

Problème d'infrastructure : pas de logs pour cette période

- Difficultés des équipes d'audit sur les sites de leurs clients
- Nécessité d'avoir un très bon contact avec les clients
- Communication très importante

Analyse possible grâce aux logs de Cooper (statistiques de Snort)

Méthodologie utilisée pendant la Phase 2

- Tri des logs de Cooper
- Identification les attaques à partir des statistiques Snort
- Recherche d'informations supplémentaires sur les attaques dans Logwatch
- Documentation sur chaque attaque
- Rédaction du rapport

Méthode d'analyse (2/3)

Présentation d'une attaque

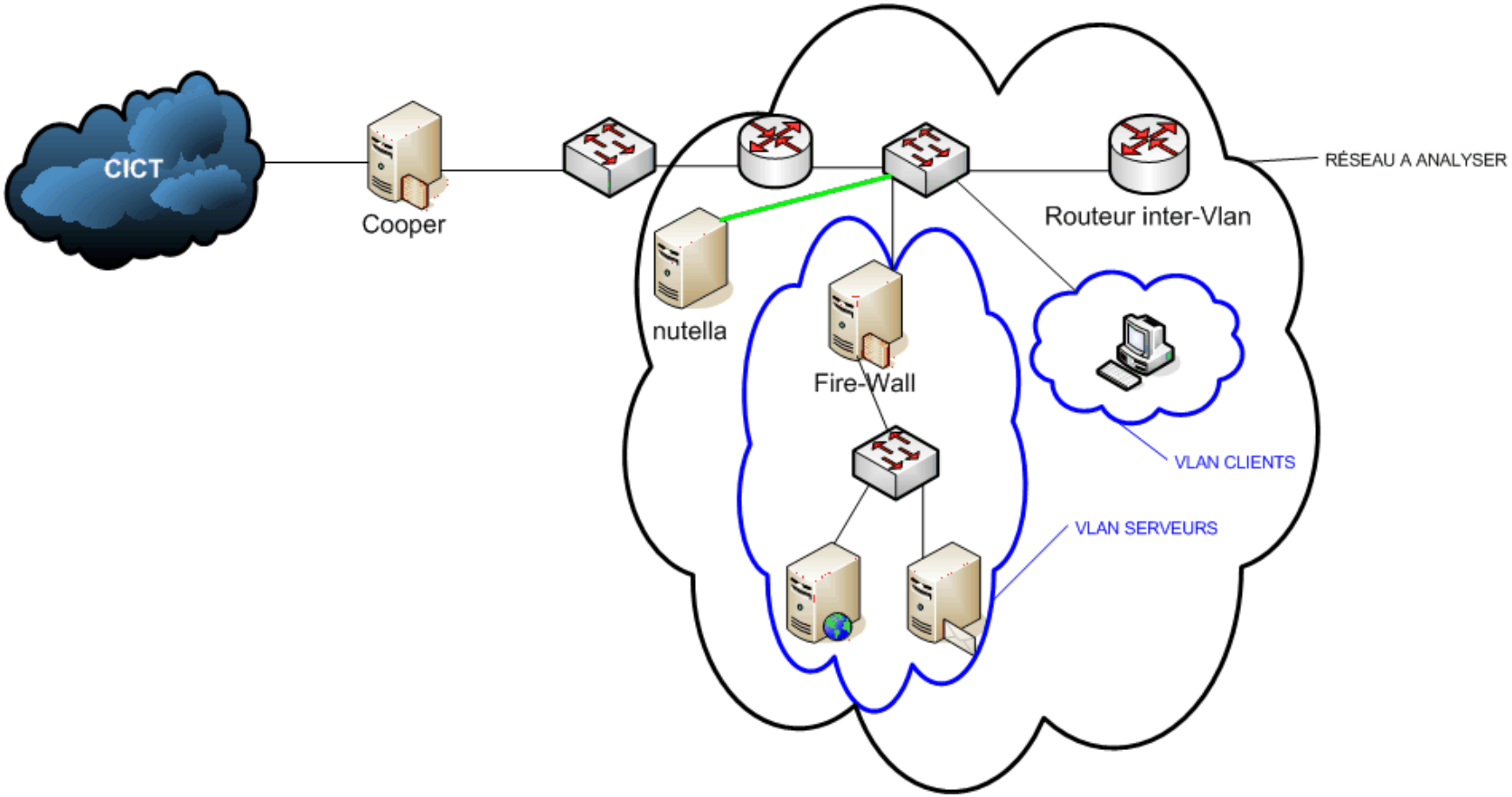
# of	from	to	method
82	172.16.80.1	172.16.80.250	ICMP redirect host
21	172.16.80.1	172.16.80.61	ICMP redirect host
14	172.16.80.71	195.220.59.7	WEB-MISC intranet access
10	172.16.80.72	195.220.59.7	WEB-MISC intranet access
5	172.16.80.61	172.16.80.1	SNMP request udp
2	172.16.80.71	212.27.42.2	WEB-CGI redirect access
2	213.186.34.205	172.66.66.6	ATTACK-RESPONSES 403 Forbidden
2	172.16.80.69	198.133.219.25	WEB-MISC /doc/ access
2	172.66.66.6	213.199.154.84	WEB-IIS %2E-asp access
2	172.77.77.100	213.199.154.84	WEB-IIS %2E-asp access
2	172.16.80.1	172.16.80.71	ICMP redirect host

Méthode d'analyse (3/3)

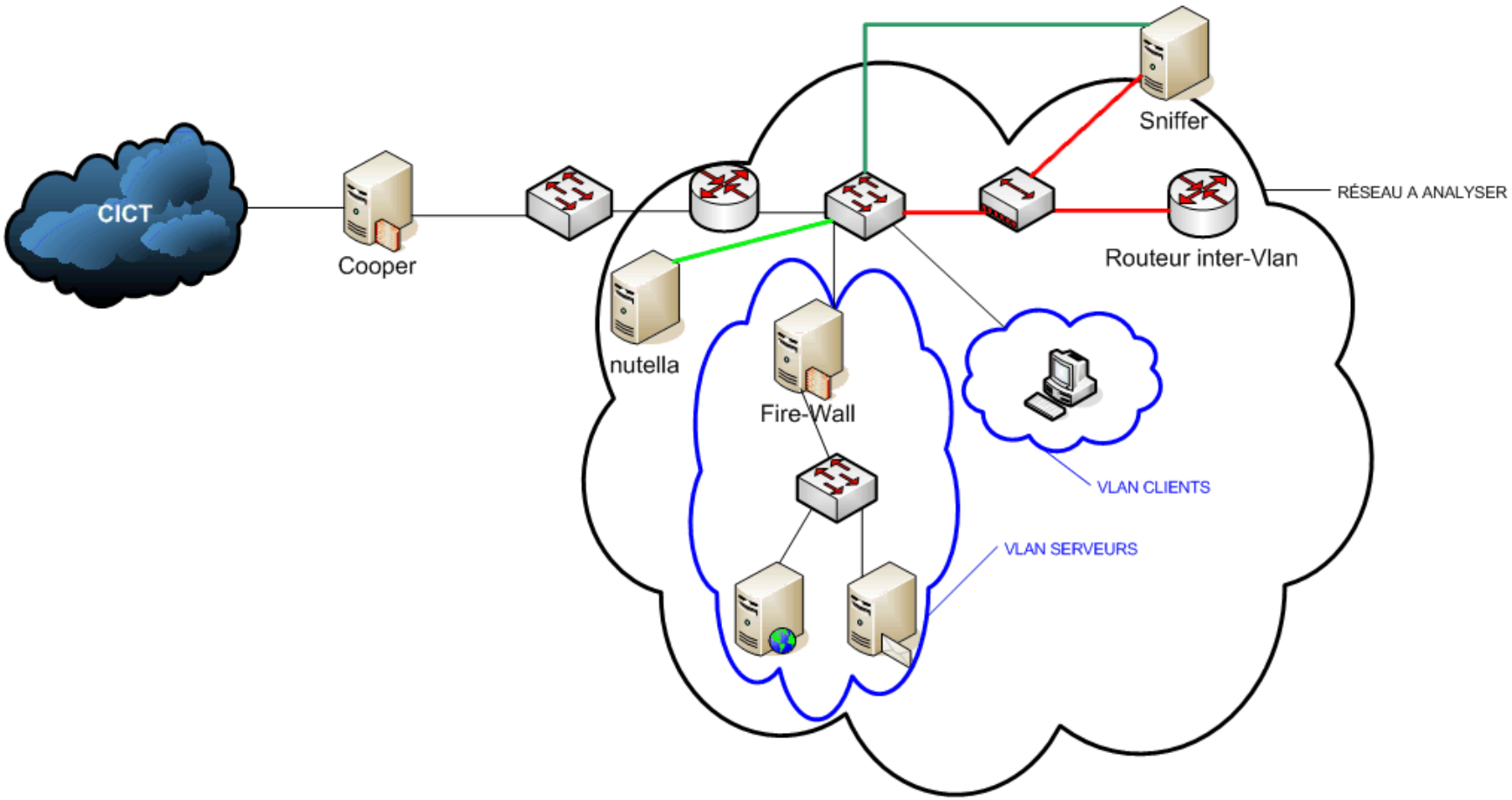
- Tentative de DNS spoofing
- Bilan de l'analyse des attaques durant la phase 2
  - Utilisation des statistiques générées par Snort
    Analyse plus rapide
  - Meilleure méthodologie
  - Les analyseurs se documentent eux mêmes sur les attaques recensées
  - Diagnostic sur chaque attaque
  - Nécessité de continuer à utiliser les méthodes de la phase 1 en parallèle

Phase 3 : Insertion d'un FireWall

Architecture (1/2)



Architecture (2/2)



Méthode d'analyse (1/2)

- Équipe d'analyse rodée
- Connaissance des attaques
- Repérage rapide des faux positifs
- Outils supplémentaires(SnortSnarf, Snort en mode démon, etc)
- Méthodologie utilisée lors de la phase 3
  - Identification des attaques à partir des statistiques Snort
  - Utilisation de Snort sur les logs collectés pour identifier les faux positifs et confirmer l'indentification
  - Fragmentation et analyse des logs pour conclure sur la réussite des attaques
  - Documentation sur chaque attaque
  - Rédaction du rapport

Méthode d'analyse (2/2)

Présentation d'une attaque

# of	from	to	method
156293	172.99.99.200	172.44.44.2	ICMP PING speedera
156293	172.99.99.200	172.44.44.2	ICMP Large ICMP Packet
139301	172.44.44.2	172.99.99.200	ICMP Large ICMP Packet

Tentative de Déni de Service sur le pot de miel(172.44.44.2)

Fructueuse?

DoS infructueux

Bilan de la phase 3

- Continuité de la phase 2
- Rapidité d'analyse des logs
- Difficultés concernant le HoneyPot

Perspectives

- Les pots de miel
- Les H-IDS
- Les IPS (Intrusion Prevention System)

Bilan du projet

Gestion du projet

- Pas de vision globale
- Manque de connaissances sur le métier
- Impossibilité d'appréhender les attaques
- Attaques irrégulières
  → Grosse charge de travail ponctuelle

→ Echéancier calé sur la défense

Communication (1/2)

En interne

- Difficulté pour attribuer des rôles précis
- Consultation quotidienne
- Efficacité de la liste de diffusion

Communication (2/2)

En externe

- Relation permanente avec la défense
  - Anticipation des changements d'architecture
  - Suivi en interne
- Ecart avec la réalité

  → Communication avec les attaquants

Apport sur les métiers

- Meilleure appréhension :
  - Échéancier
  - Vision globale des tâches
  - Importance de la communication
  - Connaissances techniques
- Les métiers : ingénieur réseau, analyste,…

Conclusion

Apport du projet

Sujet intéressant professionnellement

- Implication importante
- Axé sur la réalité du monde du travail
  - Travail en groupe
  - Sujet actuel

Améliorations envisageables pour le projet

- Plus d'informations sur les tâches
- Accès trop limité aux machines

Merci pour votre attention!

Si vous avez des questions…
(Pinguins go away !!!)