

Les Critères Communs appliqués

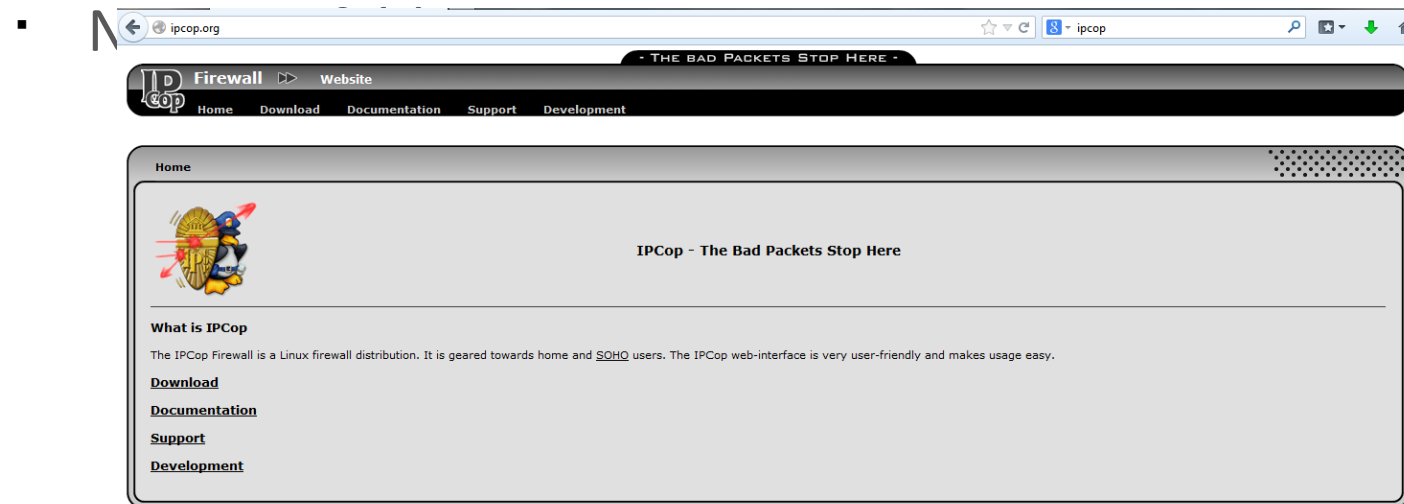
Christophe BLAD
(OPPIDA)

Agenda

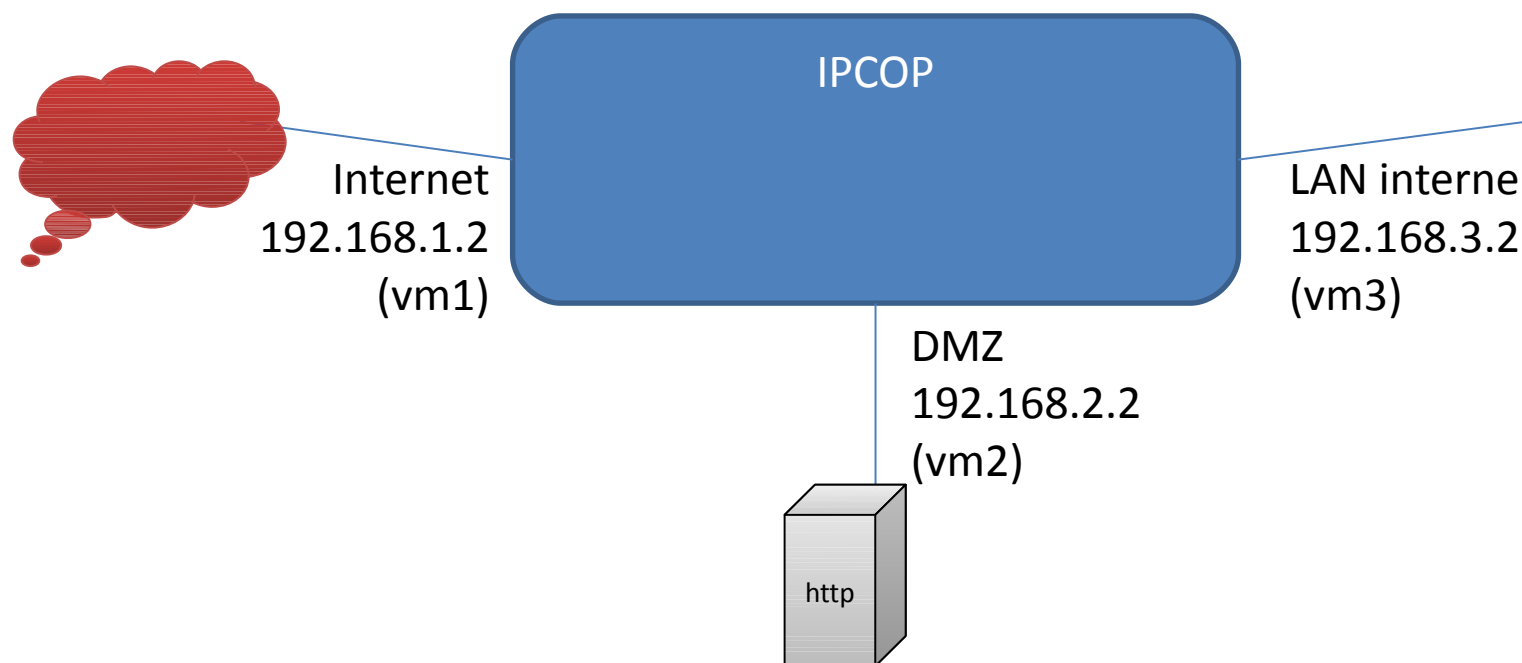
- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

L'exemple concret

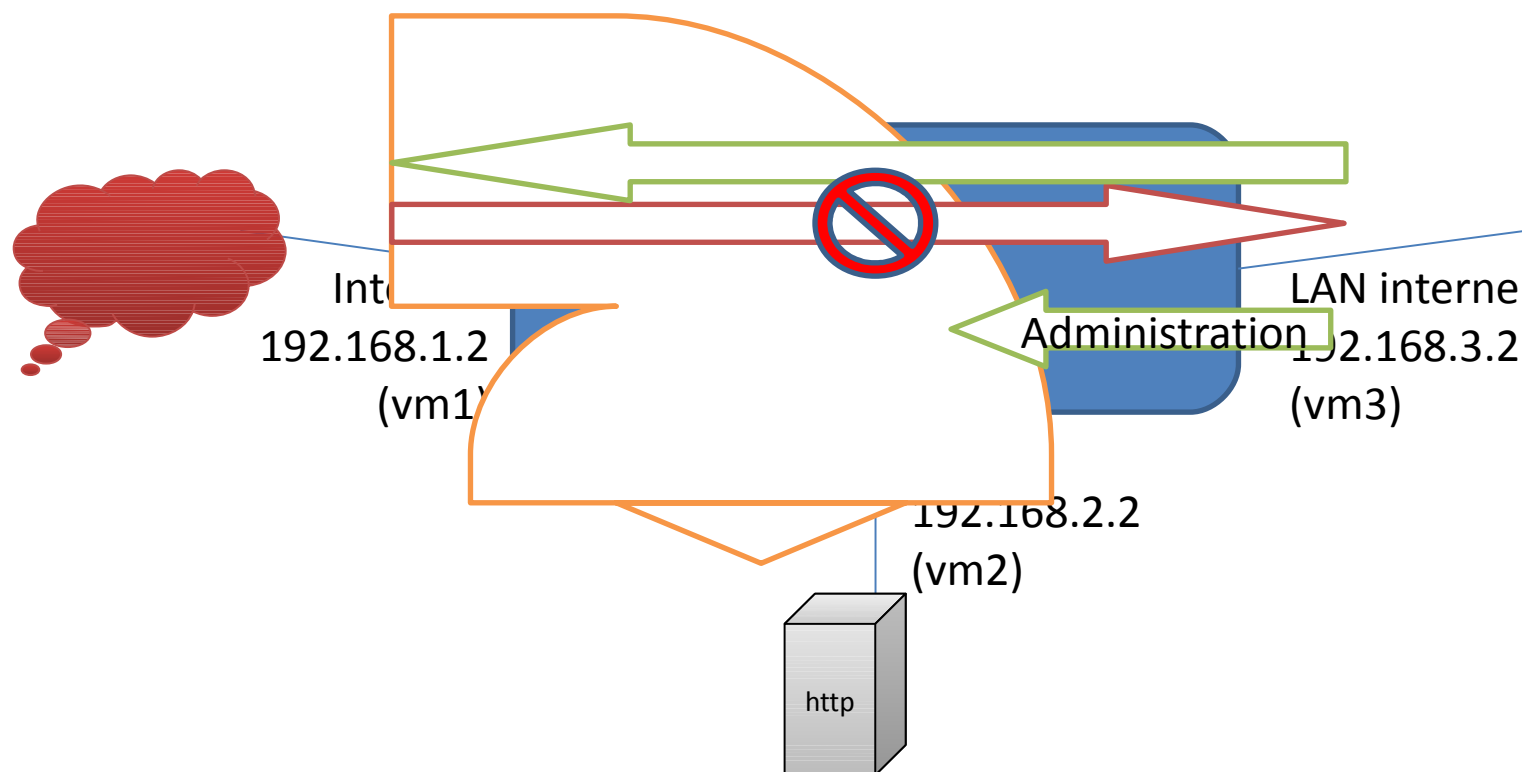
- Firewall logiciel IPCOP v2.0.3
- Open source (ipcop.org)



L'exemple concret



L'exemple concret



Agenda

- ▪ Quelques rappels
 - Rédiger une cible de sécurité
 - Analyser le process de développement
 - Analyser des spécifications fonctionnelles
 - Analyser des documents de conception
 - Analyser le code source
 - Tests fonctionnels
 - Tests de vulnérabilités

Assurance sécurité

■ **Qualité**

Caractéristiques subjectives
Non mesurables
Dépendantes des besoins

Sécurité

Expression des besoins



Exigences formalisées

Exigences fonctionnelles de sécurité [CC]

SFR: Security Functional Requirements

- **Assurance Sécurité:** Éléments de confiance que la cible de l'évaluation satisfasse les exigences fonctionnelles de sécurité. [CC v3.1]

Assurance sécurité

- Verdict d'une évaluation d'assurance sécurité: conformité aux exigences présentes dans le document *Cible de sécurité*

CONFORME

NON CONFORME

« SUCCESS »

« FAIL »

- Niveau d'assurance

- CSPN, ITSEC E1..6, CC EAL1..7

- Quantité d'information utilisée par l'évaluateur pour formuler ce

Méthodologies d'évaluation d'assurance sécurité

- ▪ CSPN: Certification Sécurité Premier Niveau
 - Produit en boîte noire:
 - le produit, sa cible de sécurité, ses guides
 - Charge imposée: 25hj pour collecter les éléments d'assurance
 - Revue des guides, reverse engineering, tests fonctionnels, analyse de vulnérabilité
 - Pas d'exhaustivité demandée
- ITSEC
 - Critères européens (1991)
 - 6 niveaux d'assurance: E1 – E6

Evaluation vs. Certification

- Evaluation (par un Centre d'évaluation: CESTI)
 - Vérifier que le produit est conforme à sa cible de sécurité
- Certification (par le bureau Certification de l'ANSSI)
 - Certifier que l'évaluation s'est déroulée dans les règles de l'art

L'évaluateur est compétent

Agrément CESTI

L'évaluateur est indépendant

- Objectifs

Statuer sur l'éligibilité du produit à être intégré dans un système de l'administration traitant des informations sensibles (mais non classifiées de Défense)

= validation préalable par le bureau qualification de l'ANSSI des exigences contenues dans les cibles de sécurité

- Trois niveaux de qualification définis dans le

RGS

- 3 parties:
 1. Introduction
 2. Catalogue d'exigences fonctionnelles
 3. Catalogue d'exigences d'assurance
- Des catalogues normalisés permettant
 - La comparaison des fonctionnalités de sécurité d'un produit évalué (partie 2)
 - La comparaison des travaux d'évaluation réalisés (partie 3)

Principaux concepts CC

- La Cible de sécurité (ST: Security Target)
 - Document décrivant:
 - Le produit à évaluer (TOE)
 - Son contexte d'emploi
 - Les fonctions de sécurité exigées (SFR)
 - Les travaux d'évaluation à réaliser (SAR)
- La cible d'évaluation (TOE: Target Of Evaluation)
 - Le produit ou le système (technique) qui est l'objet de l'évaluation
- 2 tâches dans une évaluation CC

Agenda

- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

La cible d'évaluation

- ▪ TOE: Target of Evaluation
IPCOP v2.0.3
- Type de TOE: firewall
- Description de la TOE: cf site web

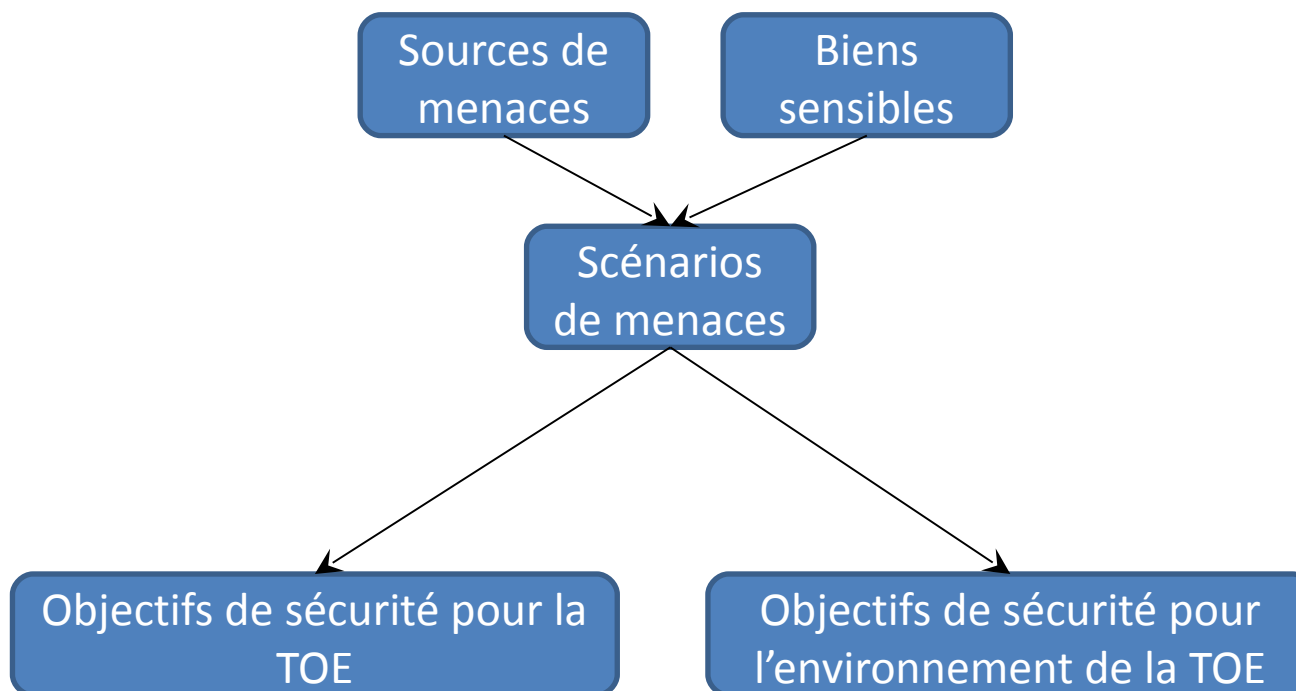
Les utilisateurs de la TOE

- Les utilisateurs/machines connectés aux réseaux interconnectés (WAN, DMZ, LAN)
- Les administrateurs du firewall

Sujets / Opérations / Objets

- ▪ Sujet / Verbe / Complément
- Le [firewall (la TOE)] [filtre] les [trames IP]
- L'[Administrateur] [configure] les [règles de filtrage]

L'analyse de risque



Sources de menaces (accident et/ou attaque)

- ▪ Les utilisateurs légitimes
 - Utilisateurs des réseaux
 - Administrateurs

- Les personnes ayant accès à la TOE
 - Technicien ayant accès à la salle serveur
 - Accès physique

 - Machine sur le WAN (utilisateurs du WAN)
 - Machine sur la DMZ (utilisateurs de la DMZ)
 - Machine sur le LAN interne (utilisateurs du LAN)

C'est le moment de faire des choix

- Les sources de menaces sont-elles retenues pour l'évaluation?
- Si non -> hypothèses

Administrateurs	NON	<i>Il est fait l'hypothèse que les administrateurs sont de confiance et bien formés</i>
Technicien ayant accès à la salle serveur	NON	<i>Il est fait l'hypothèse que l'accès physique à la TOE est limité à des personnes de confiance</i>
Machine sur le WAN	OUI	
Machine sur la DMZ	OUI	
Machine sur le LAN	OUI	

Les biens sensibles

- ▪ Les données protégées par la TOE (User-data)
 - Le serveur web protégé par le firewall
 - Le réseau interne

- Les données de la TOE elle-même (TSF-data)
 - Les règles de filtrage

Scénarios de menaces

	Le serveur web	Le réseau interne	Les règles de filtrage
Machine sur le WAN	Intrusion serveur web à partir WAN	Intrusion réseau interne à partir WAN	Intrusion TOE à partir WAN
Machine sur la DMZ	Hors périmètre	Intrusion réseau interne à partir DMZ	Intrusion TOE à partir DMZ
Machine sur le LAN	Non retenu	Hors périmètre	Intrusion TOE Attaque du compte administrateur

Objectifs de sécurité

	Objectifs pour la TOE	Objectifs pour l'environnement de la TOE
Intrusion serveur web à partir WAN	Filtrage trames traversantes Journalisation	
Intrusion réseau interne à partir WAN	Filtrage trames traversantes Journalisation	
Intrusion TOE à partir WAN	Filtrage trames entrantes Journalisation	
Intrusion réseau interne à partir DMZ	Filtrage trames traversantes Journalisation	
Intrusion TOE à partir DMZ	Filtrage trames entrantes Journalisation Filtrage trames entrantes	
Intrusion TOE à partir LAN	Journalisation Authentification administrateur	Administrateur ne doit pas communiquer son mot de passe
Attaque compte administrateur		
		Procédures d'habilitation et de formation des administrateurs
Administrateurs de confiance	Les Critères Communs appliqués	TOE doit être installée dans une salle à accès contrôlé

C'est là que ca pique ...

- Traduction des objectifs sur la TOE dans le langage CC
- Langage naturel -> Exigences communes extraites de la partie 2

	Exigences CC Part 2
Filtrage trames traversantes	FDP_IFC.1, FDP_IFF.1 / trames traversantes
Filtrage trames entrantes	FDP_IFC.1, FDP_IFF.1 / trames entrantes
Journalisation	FAU_GEN.1
Authentification administrateur	FIA_UAU.1

Juste un exemple: Politique de contrôle de flux traversants

- ▪ FDP_IFC.1
 - FDP_IFC.1.1 The TSF shall enforce the [*Politique filtrage flux traversants*] on [*Trames IP*].

- FDP_IFF.1
 - FDP_IFF.1.1 The TSF shall enforce the [*Politique filtrage flux traversants*] based on the following types of subject and information security attributes:

[Trames IP: *adresse/port source, adresse/port destination*].

- FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

Politique de contrôle de flux traversants

1. ALLOW + LOG

source_IP = 192.168.1.*, (wan)

source_port = *,

destination_IP = 192.168.2.127, (serveur web)

Destination_port = tcp 80 (http)

2. ALLOW + LOG

source_IP = 192.168.3.*, (lan)

source_port = *,

destination_IP = 192.168.1.*, (wan)
appliqués

Politique de contrôle de flux entrants

1. ALLOW + LOG

source_IP = 192.168.3.*, (lan)

source_port = *,

destination_IP = 192.168.3.2, (TOE)

Destination_port = tcp 8443 (https)

2. DENY ALL

Résumé des spécifications fonctionnelles

	TOE
FDP_IFC.1, FDP_IFF.1 / trames traversantes	Filtrage à l'aide du programme iptables (règles FORWARD)
FDP_IFC.1, FDP_IFF.1 / trames entrantes	Filtrage à l'aide du programme iptables (règles INPUT)
FAU_GEN.1	Journalisation syslog
FIA_UAU.1	Authentification par login / mot de passe

Agenda

- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

ALC: évaluation du cycle de vie de la TOE

- ▪ Modèle de cycle de développement (ALC_LCD)
 - Produit open-source
 - Production de release

- Gestion de configuration (ALC_CMC, ALC_CMS)
 - Tout (code source + documentation) dans un dépôt Subversion chez SourceForge

- Sécurité de l'environnement de développement (ALC_DVS)

Agenda

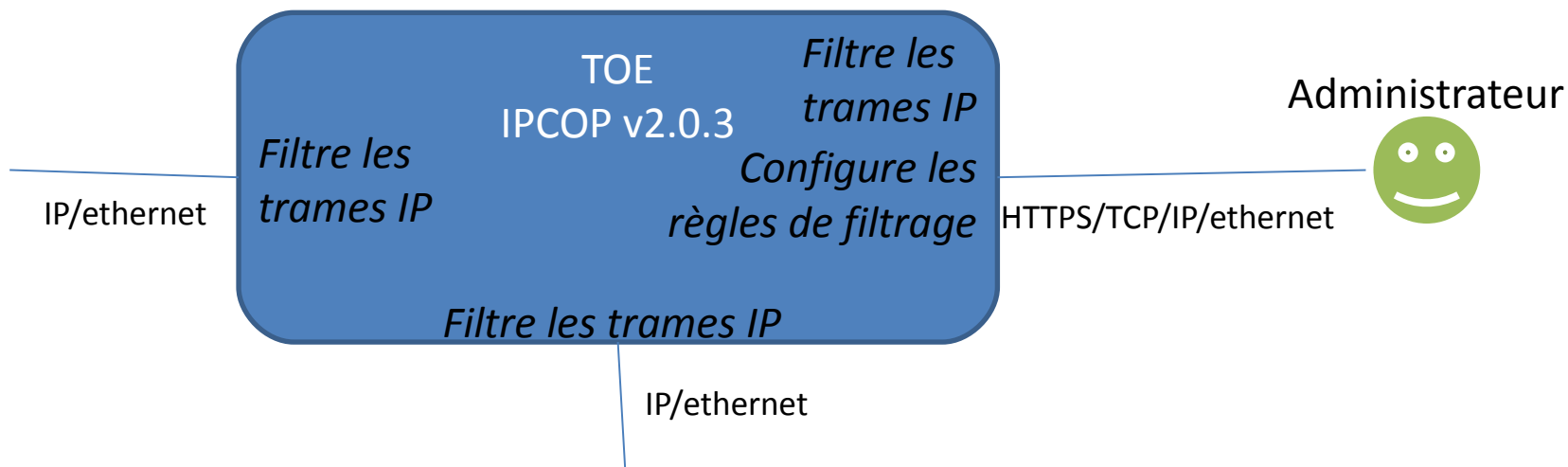
- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

- ▪ Objectifs
 - Comprendre les moyens d'interagir avec la TOE
 - Comprendre quand sont déclenchées les fonctions de sécurité?

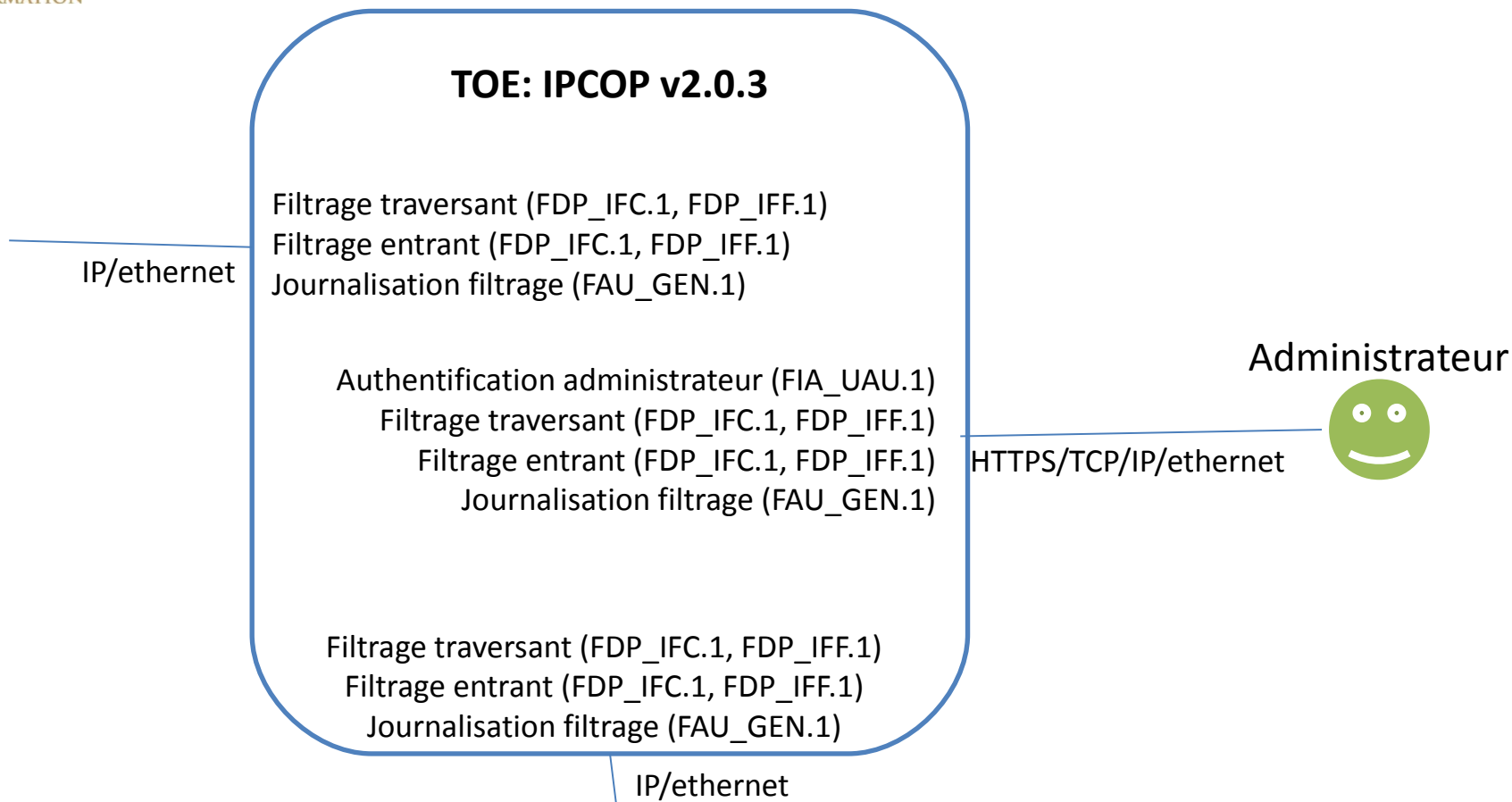
- Données d'entrée
 - Documents de spécifications fonctionnelles fournis par le développeur de la TOE

ADV_FSP: Interfaces et actions

- ▪ Rappelez-vous les Sujets/Opérations/Objets



ADV_FSP: mapping avec les exigences fonctionnelles



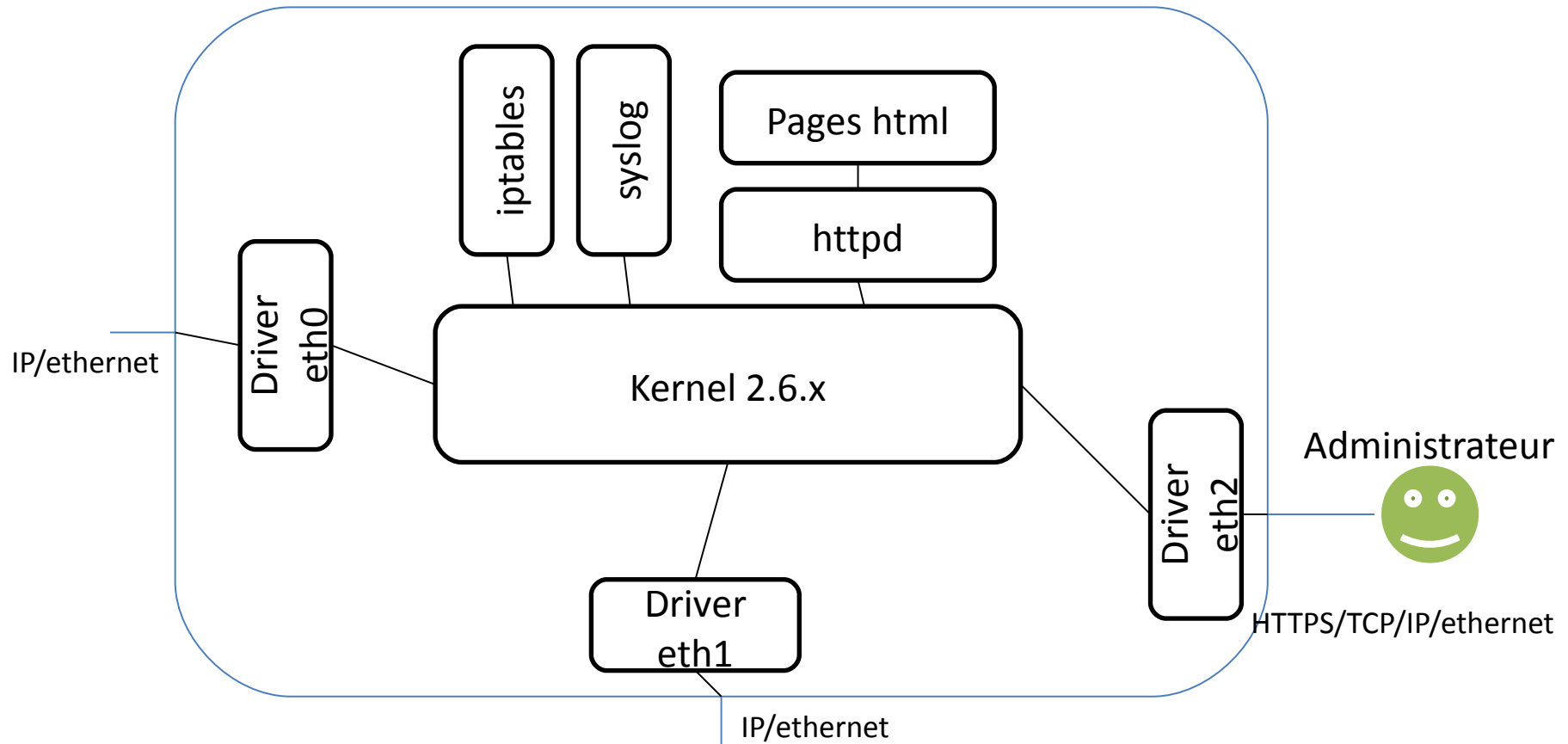
Agenda

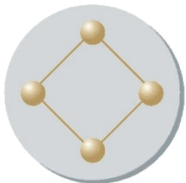
- - Quelques rappels
 - Rédiger une cible de sécurité
 - Analyser des spécifications fonctionnelles
 - Analyser des documents de conception
 - Analyser le code source
 - Tests fonctionnels
 - Tests de vulnérabilités

- ▪ Objectifs
 - Comprendre l'architecture de la TOE
 - Identifier où sont implémentées les fonctions de sécurité

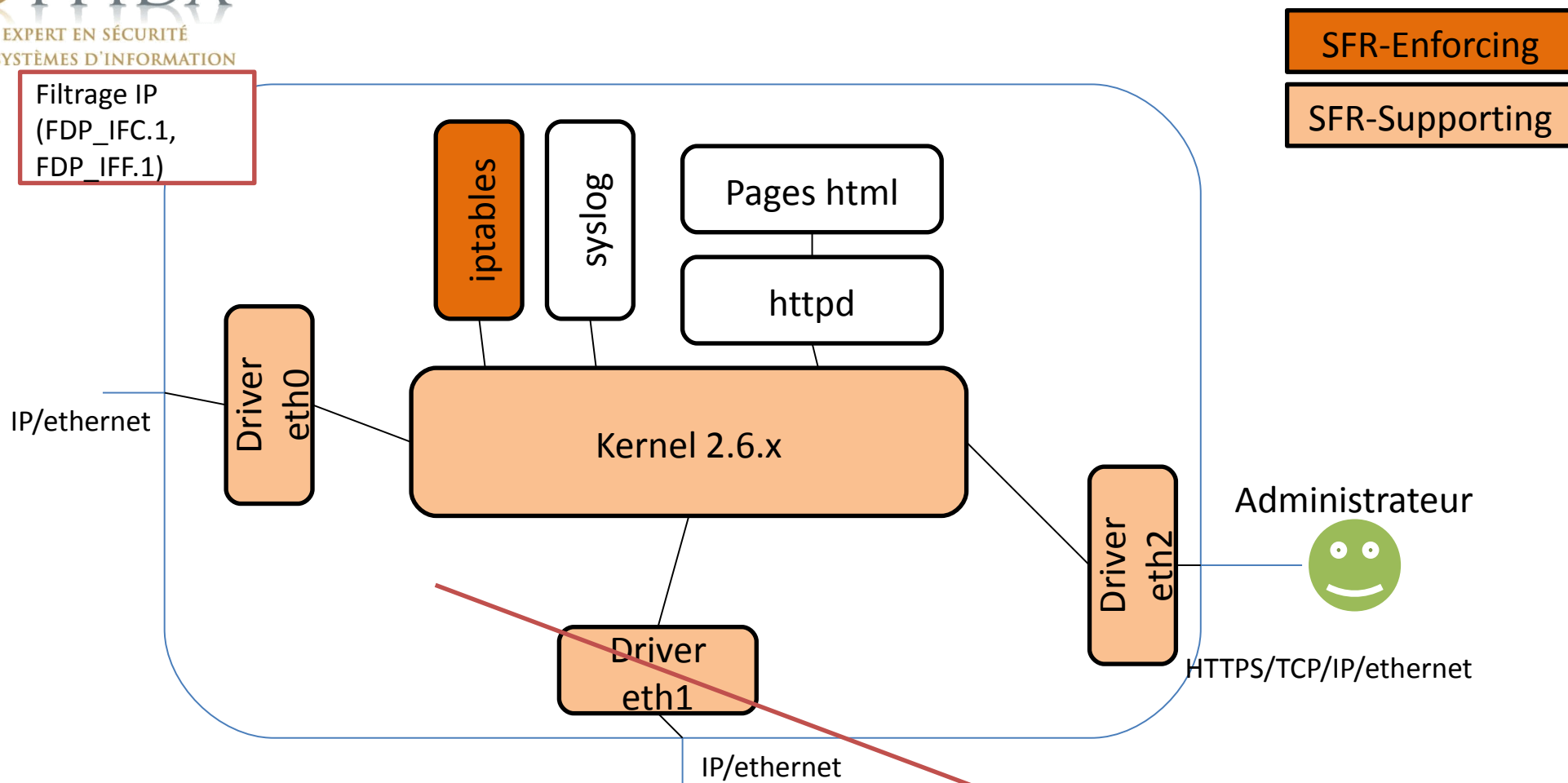
- Données d'entrée
 - Documents de description de la conception de la TOE fournis par le développeur

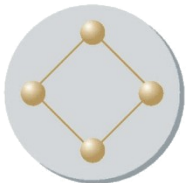
ADV_TDS: décomposition en sous-systèmes et modules



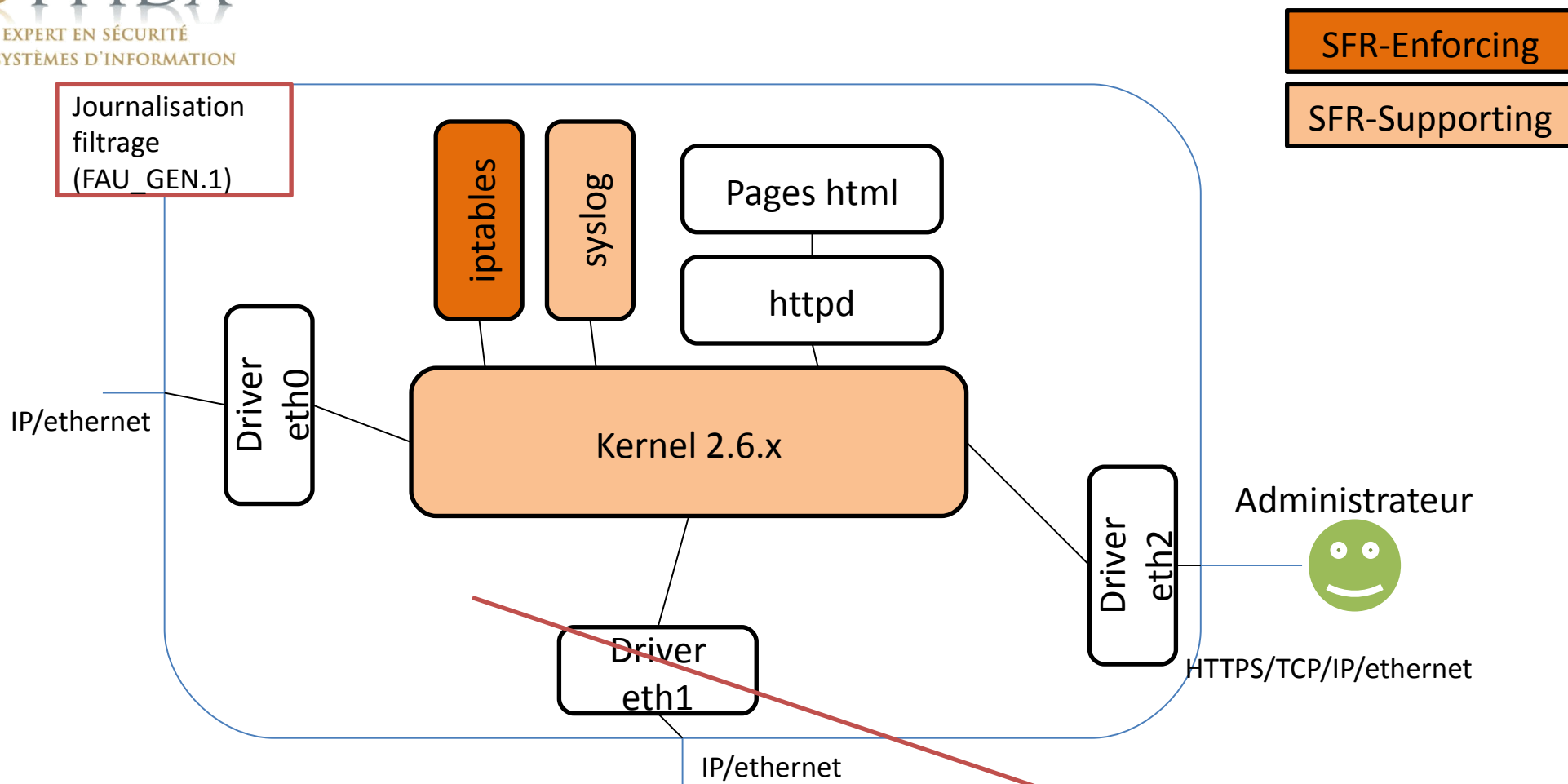


Délimitation de la TSF: Filtrage IP

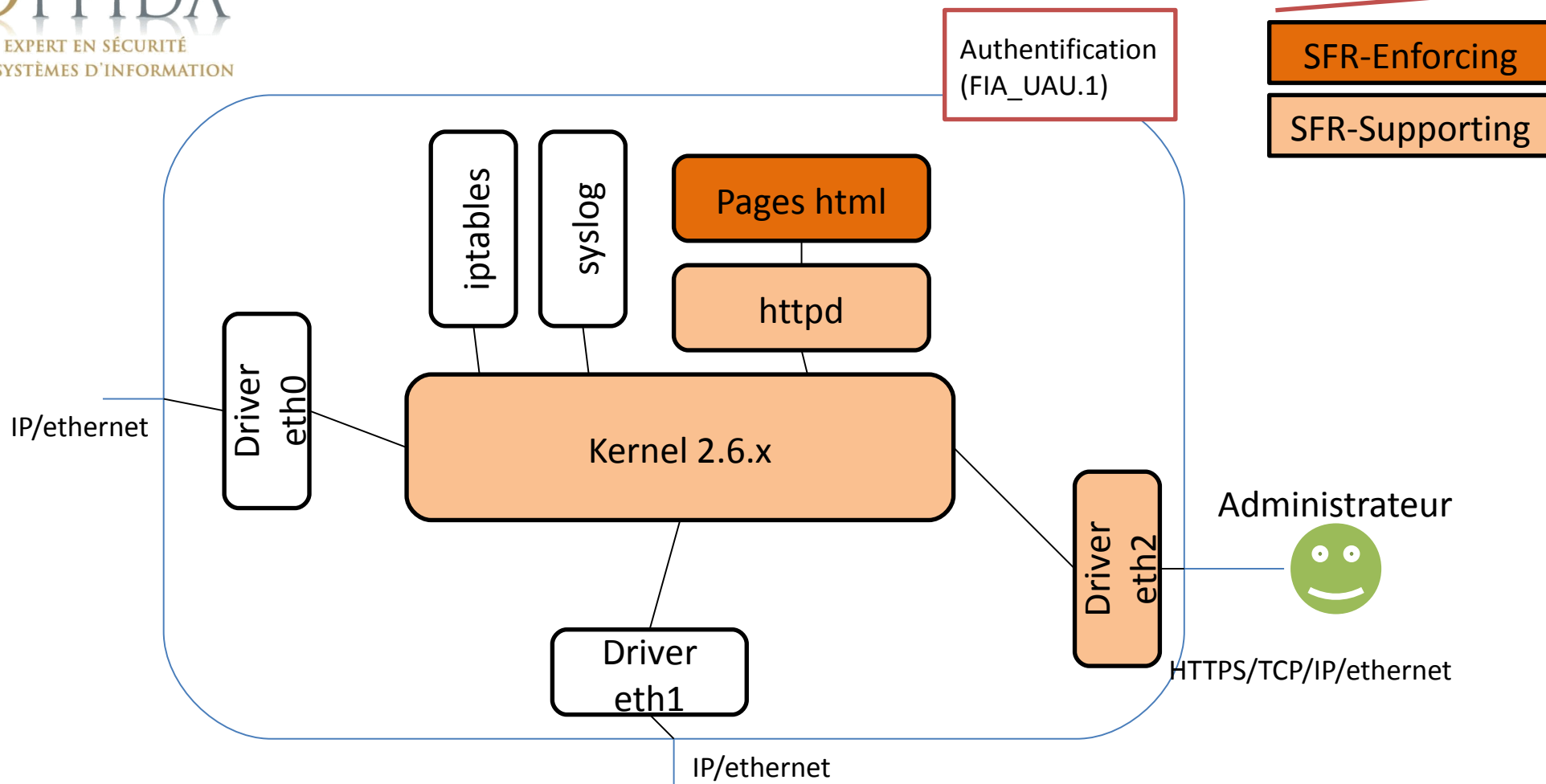




Délimitation de la TSF: Journalisation



Délimitation de la TSF: Authentification



Agenda

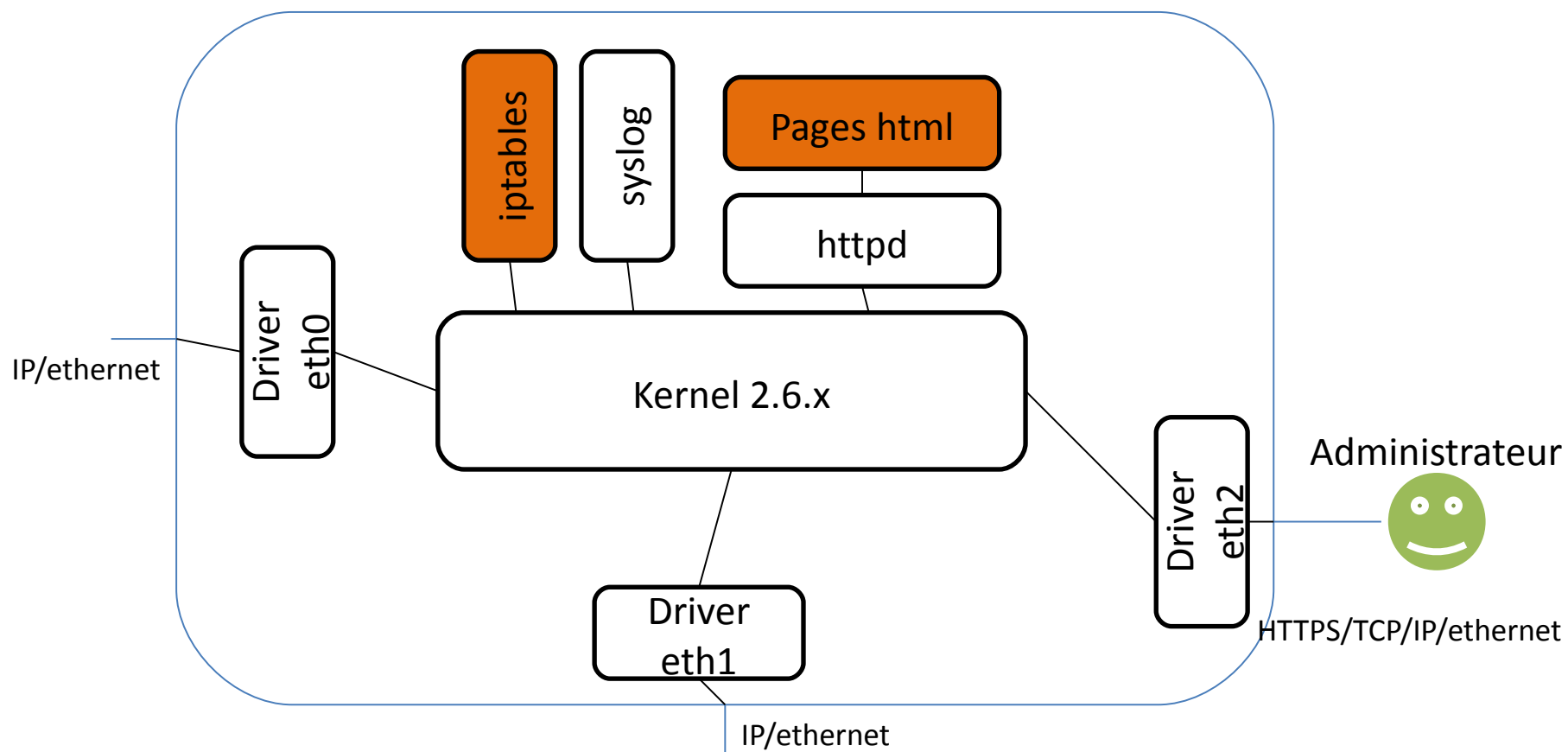
- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le process de développement
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

ADV_IMP: TSF implementation

- ▪ Conformité
 - Vérifier la réalisation effective des SFR
 - Code source
 - Configuration
- À partir du niveau EAL4 seulement

ADV_IMP: TSF implementation

SFR-Enforcing



ADV_IMP: TSF implementation

- ▪ Filtrage & journalisation
 - Réalisation dépend de la configuration: `iptables -L`

- Authentification
 - Réalisation dans le code source: scripts `cgi`

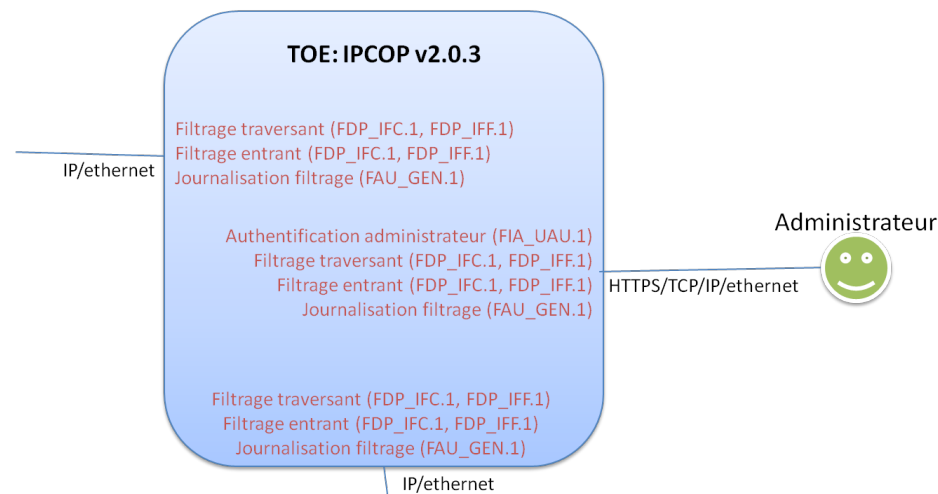
Agenda

- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

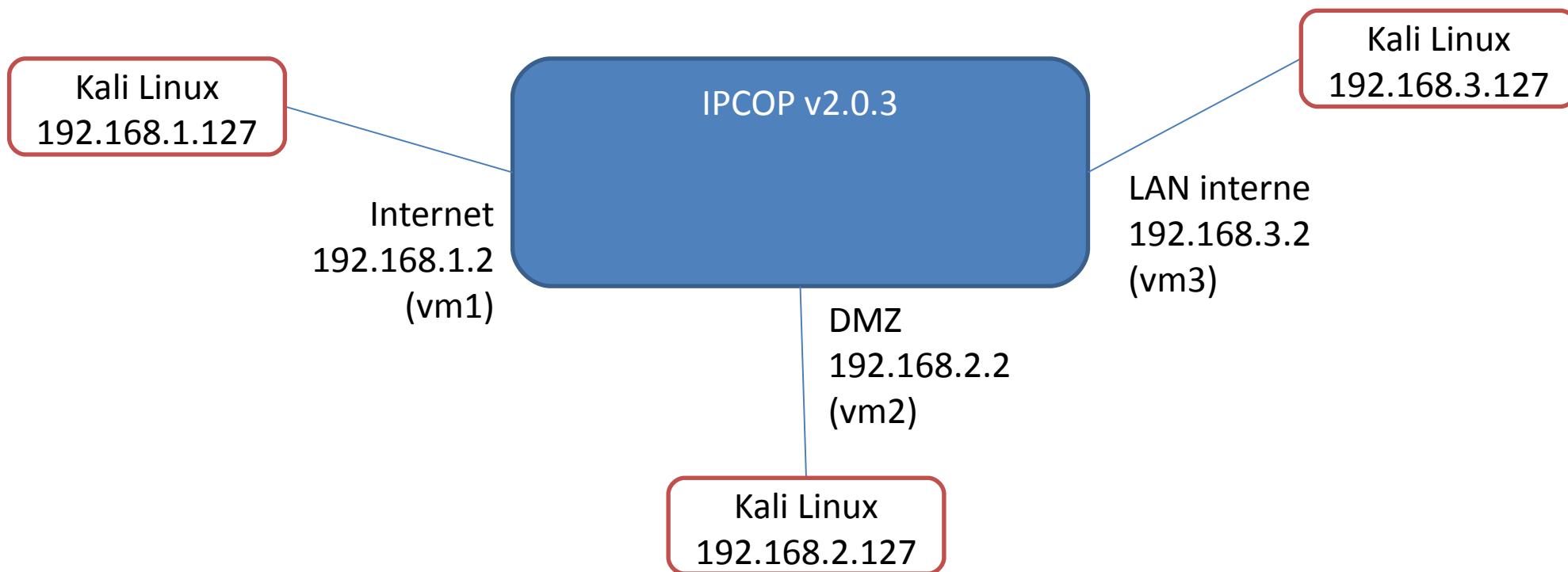
- 1. Valider le plan de tests du développeur
- 2. Réaliser des tests indépendants
 - 1. Rejeu d'une partie des tests fournis par le développeur
 - 2. Elaboration de nouveaux tests

Plan de tests fonctionnels

- Vérifier [Filtrage traversant] sur [Interface WAN]
- Vérifier [Filtrage entrant] sur [Interface WAN]
- Vérifier [Journalisation filtrage] sur [Interface WAN]
- Vérifier [Filtrage traversant] sur [Interface DMZ]
- Vérifier [Filtrage entrant] sur [Interface DMZ]



Plateforme de tests



Agenda

- ▪ Quelques rappels
- Rédiger une cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

Organisation de l'analyse de vulnérabilités

- 1. Vulnérabilités connues
- 2. Analyse indépendante de vulnérabilités
 - 1. Brainstorming, base de connaissances
 - 2. Tests

Vulnérabilités connues

- - Pour le produit
 - Pour des composants du produit
 - Base CVE
 - cvedetails.com
 - [Securityfocus](http://securityfocus.com)
 - ...

cvedetails

CVE Details

The ultimate security vulnerability datasource

Google™ Custom Search

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View CVE

Vulnerability Feeds & Widgets^{New}

www.itsecdb.com



[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

[Feedback](#)

[CVE Help](#)

[FAQ](#)

[Articles](#)

External Links :

[Ipcop](#) » [Ipcop](#) : Vulnerability Statistics

[Vulnerabilities \(3\)](#) [CVSS Scores Report](#) [Browse all versions](#) [Possible matches for this product](#) [Related Metasploit Modules](#)

[Related OVAL Definitions](#) : [Vulnerabilities \(0\)](#) [Patches \(0\)](#) [Inventory Definitions \(0\)](#) [Compliance Definitions \(0\)](#)

[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

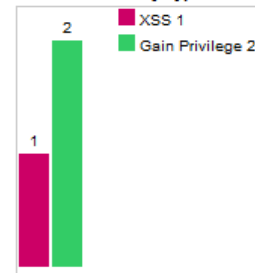
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	3						1					2			
Total	3						1					2			
% Of All		0.0	0.0	0.0	0.0	0.0	33.3	0.0	0.0	0.0	0.0	66.7	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type

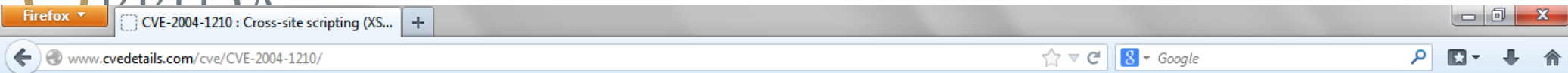


Les Critères Communs
appliqués

FR

23:49
20/01/2014

XSS



CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widgets^{New}

www.itsecdb.com



[Home](#)

Browse :

[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)
[CVSS Score Distribution](#)

Search :

[Vendor Search](#)
[Product Search](#)
[Version Search](#)
[Vulnerability Search](#)
[By Microsoft References](#)

Top 50 :

[Vendors](#)
[Vendor Cvss Scores](#)
[Products](#)
[Product Cvss Scores](#)
[Versions](#)

Other :

[Microsoft Bulletins](#)
[Bugtraq Entries](#)
[CWE Definitions](#)
[About & Contact](#)
[Feedback](#)
[CVE Help](#)
[FAQ](#)
[Articles](#)

Vulnerability Details : [CVE-2004-1210](#)

Cross-site scripting (XSS) vulnerability in proxylog.dat in IPCop 1.4.1 and possibly other versions, allows remote attackers to inject arbitrary web script or HTML via the (1) url or (2) part variables.

Publish Date : 2005-01-10 Last Update Date : 2008-09-05

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	6.8
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	User
Vulnerability Type(s)	Cross Site Scripting
CWE ID	CWE id is not defined for this vulnerability

- Products Affected By CVE-2004-1210

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Ipcop	Ipcop	1.4.1			Version Details Vulnerabilities

- Number Of Affected Versions By Product

Les Critères Communs
appliqués

Via backup



Firefox | Ipcop Ipcop : List of security vulnerabilities | www.cvedetails.com/vulnerability-list/vendor_id-2654/product_id-4640/year-2005/opgpriv-1/lpcop-Ipcop.html

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

[Vulnerability Feeds & Widgets^{New}](#) www.itsecdb.com

- [Home](#)
- Browse :**
 - [Vendors](#)
 - [Products](#)
 - [Vulnerabilities By Date](#)
 - [Vulnerabilities By Type](#)
- Reports :**
 - [CVSS Score Report](#)
 - [CVSS Score Distribution](#)
- Search :**
 - [Vendor Search](#)
 - [Product Search](#)
 - [Version Search](#)
 - [Vulnerability Search](#)
 - [By Microsoft References](#)
- Top 50 :**
 - [Vendors](#)
 - [Vendor Cvss Scores](#)
 - [Products](#)
 - [Product Cvss Scores](#)
 - [Versions](#)
- Other :**
 - [Microsoft Bulletins](#)
 - [Bugtraq Entries](#)
 - [CWE Definitions](#)
 - [About & Contact](#)
 - [Feedback](#)
 - [CVE Help](#)
 - [FAQ](#)

[Ipcop](#) » [Ipcop](#) : Security Vulnerabilities Published In 2005 (Gain Privilege)

2005 : [January](#) [February](#) [March](#) [April](#) [May](#) [June](#) [July](#) [August](#) [September](#) [October](#) [November](#) [December](#) CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2005-4660			+Priv	2005-12-31	2008-09-05	1.2	None	Local	High	Not required	None	Partial	None
Race condition in IPCop (aka IPCop Firewall) before 1.4.10 might allow local users to overwrite system configuration files and gain privileges by replacing a backup archive during the time window when the archive is owned by "nobody" but not yet encrypted, then executing ipcoprscfg to restore from this backup.														
2	CVE-2005-4659			+Priv	2005-12-31	2008-09-05	2.1	None	Local	Low	Not required	Partial	None	None
IPCop (aka IPCop Firewall) before 1.4.10 has world-readable permissions for the backup.key file, which might allow local users to overwrite system configuration files and gain privileges by creating a malicious encrypted backup archive owned by "nobody", then executing ipcoprscfg to restore from this backup.														

Total number of vulnerabilities : 2 Page : 1 (This Page)

Les Critères Communs
appliqués

Tests de vulnérabilités

- ▪ Définir les points d'attaque
 - WAN
 - DMZ
 - LAN

- Méthodologie tests d'intrusion
 - Collecte d'information
 - Recherche de points faibles
 - Attaque / intrusion

Cotation de l'attaque

- ▪ Besoin d'évaluer le niveau de complexité de l'attaque
- Permet d'en déduire le niveau de résistance de la TOE
 - AVA_VAN.1: résistance aux CVE publiées
 - AVA_VAN.2: résistance aux attaques de niveau *basic* (boite noire)
 - AVA_VAN.3: résistance aux attaques de niveau *enhanced-basic* (avec le code source)
 - AVA_VAN.4: résistance aux attaques de niveau *moderate*
 - AVA_VAN.5: résistance aux attaques de niveau *high*

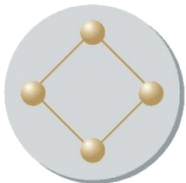
Table de cotation des attaques: CEM

- ▪ CEM annexe B.4 (p428/433)
- *Elapsed Time*: temps passé à trouver + exploiter la vulnérabilité
- *Expertise*: type de compétence nécessaire (identification et exploitation)
- *Knowledge of TOE*: connaissance du produit nécessaire
- *Window of Opportunity*: difficulté d'accès au produit
- *Equipment*: type d'outil nécessaire (identification et exploitation)

Dans notre exemple

■ ▪ Brute-force SSH

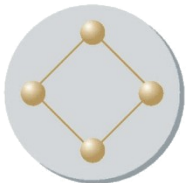
Facteur	Valeur	Cotation
Elapsed Time	10 minutes (< 1 day)	0
Expertise	Compétent (proficient)	3
Knowledge of TOE	Adresse IP (public)	0
Window of Opportunity	Accès au WAN + connectivité IP (easy)	1
Equipment	Spécialisé (specialised)	4



Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1 , AVA_VAN.2 , AVA_VAN.3 , AVA_VAN.4 , AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1 , AVA_VAN.2	AVA_VAN.3 , AVA_VAN.4 , AVA_VAN.5
14-19	Moderate	Enhanced	AVA_VAN.1	AVA_VAN.4

Cotation des vulnérabilités

- ▪ Liste des vulnérabilités trouvées dans le Rapport Technique d'Evaluation (mais pas dans la partie publique: le rapport de certification)
- Vulnérabilité exploitable
 - Pas de certificat
- Vulnérabilité résiduelle
 - Niveau de complexité de l'attaque > niveau AVA_VAN demandé



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Des questions ?

OPPIDA recrute

- pentest
- expertise technique de produits
- évaluations CSPN, ITSEC, CC

Conseil & Expertise
en sécurité des systèmes d'information



contact@oppida.fr