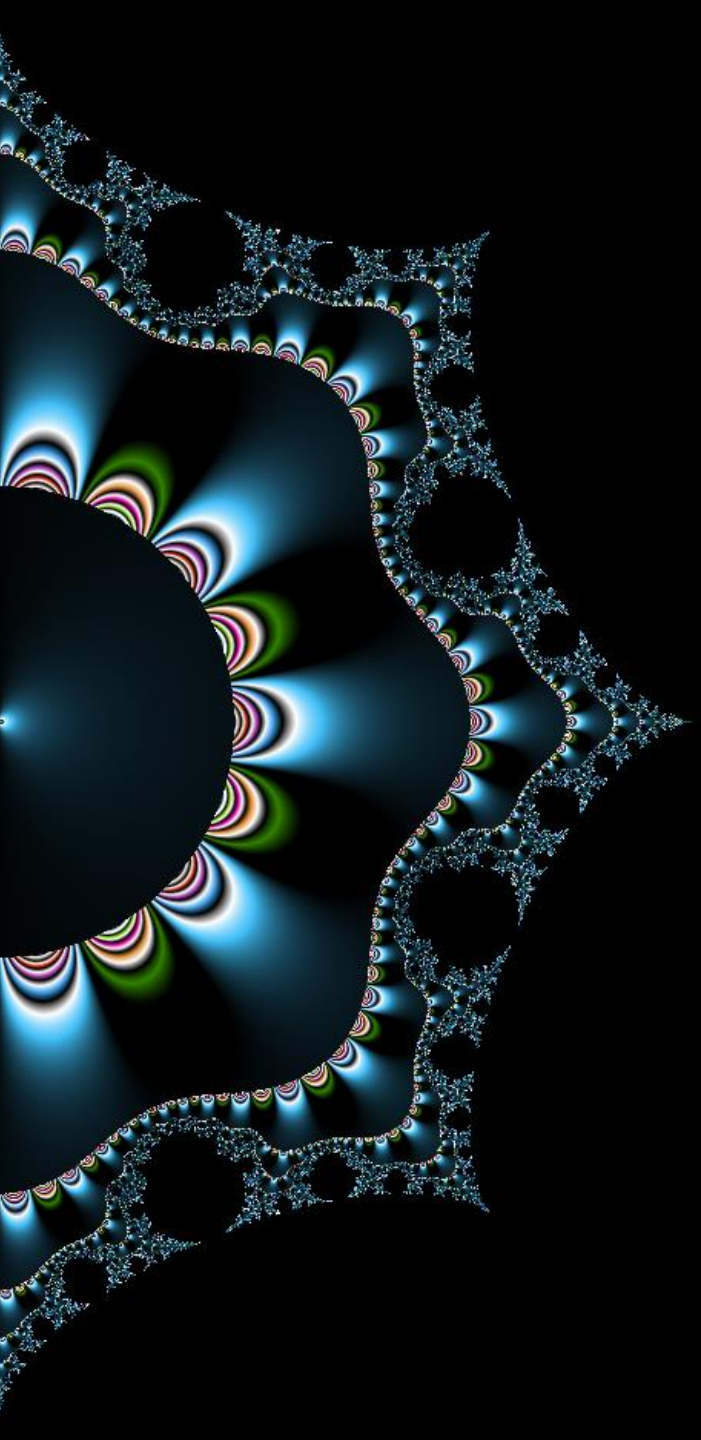


DNS

Prélude à tout le web

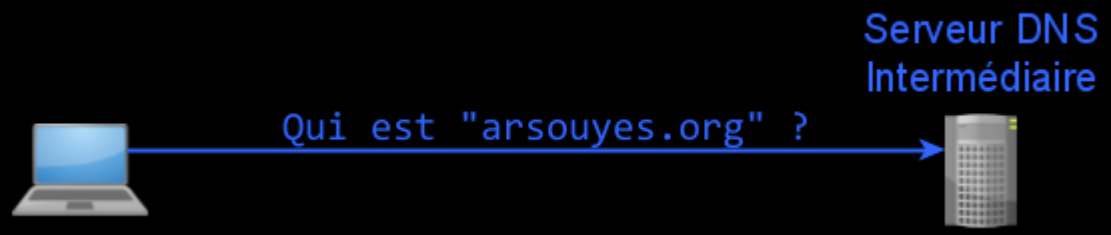
Thibaut HENIN

tbowan@arsouyes.org

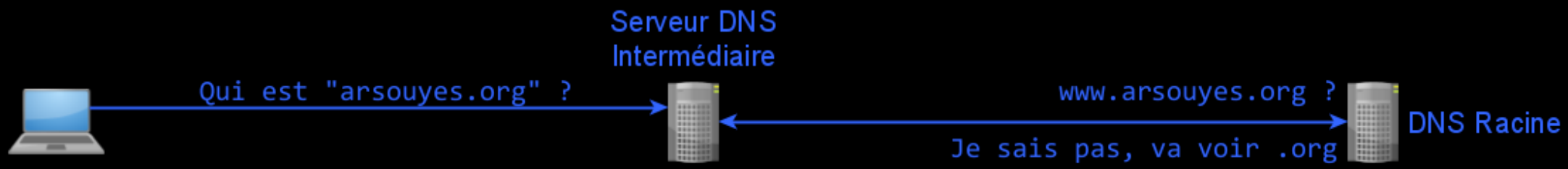
Principes de fonctionnement

Simple mais complexe

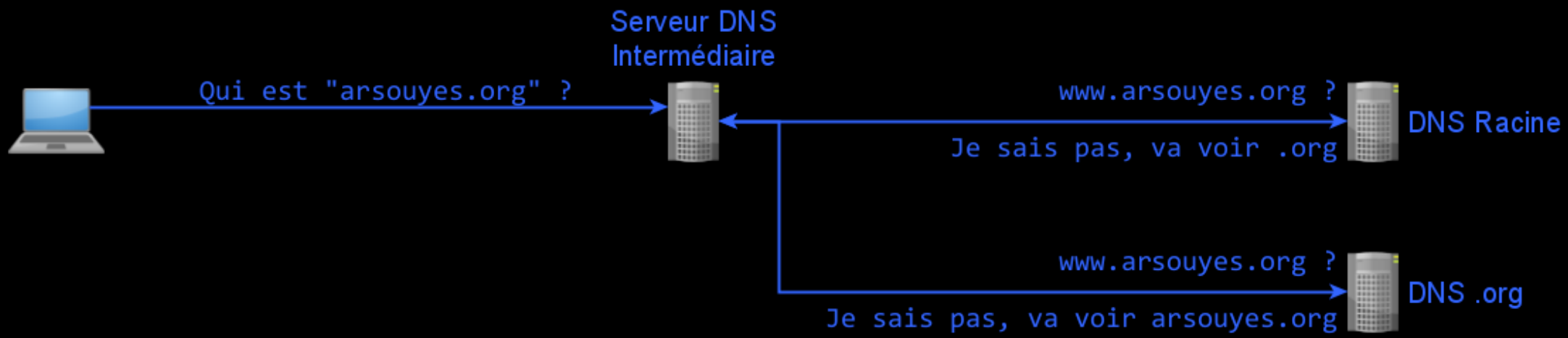
Requête DNS



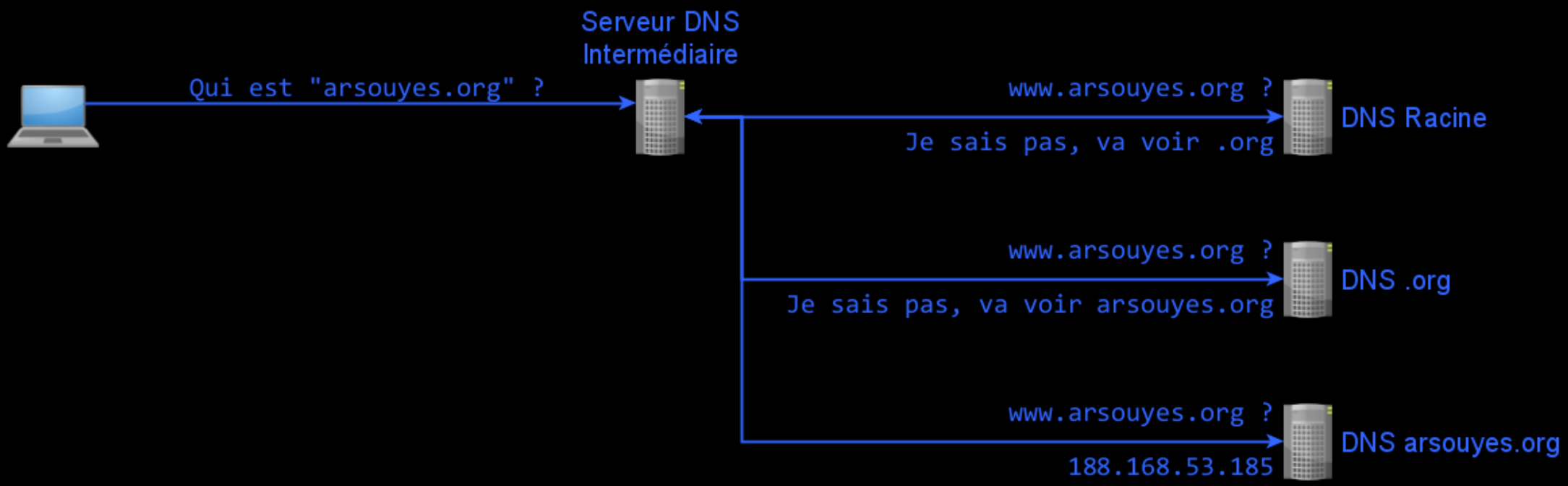
Requête DNS


Serveur DNS
Intermédiaire
Qui est "arsouyes.org" ?
www.arsouyes.org ?
Je sais pas, va voir .org
DNS Racine

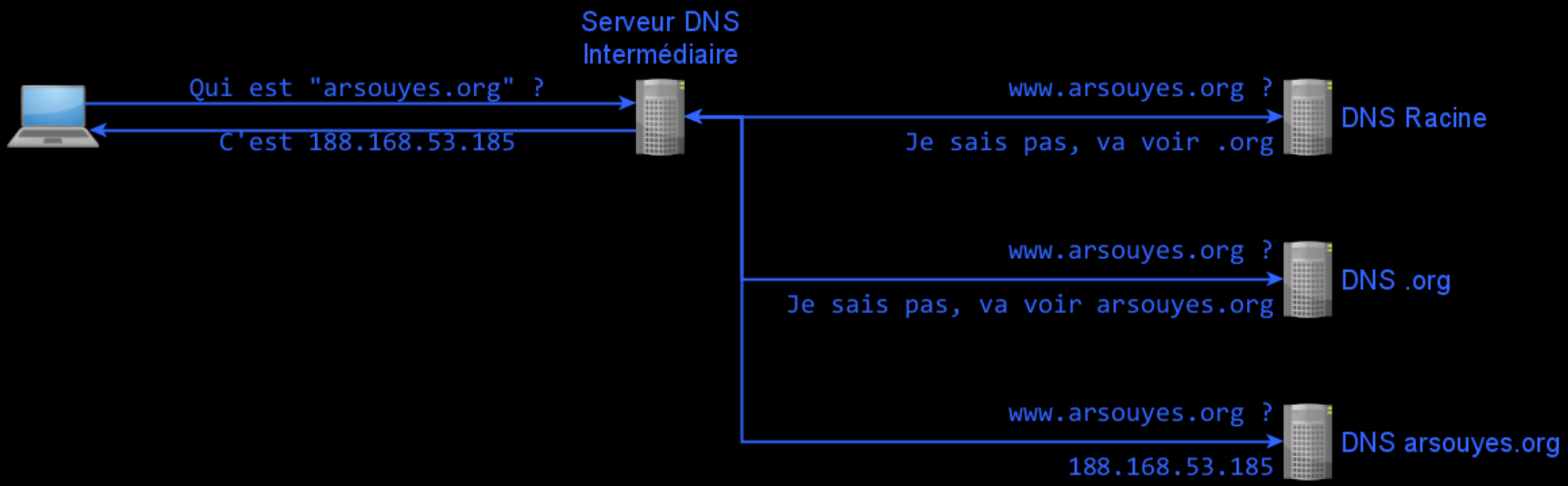
Requête DNS


Serveur DNS
Intermédiaire
Qui est "arsouyes.org" ?
www.arsouyes.org ?
Je sais pas, va voir .org
DNS Racine
www.arsouyes.org ?
Je sais pas, va voir arsouyes.org
DNS .org

Requête DNS


Serveur DNS
Intermédiaire
Qui est "arsouyes.org" ?
www.arsouyes.org ?
Je sais pas, va voir .org
DNS Racine
www.arsouyes.org ?
Je sais pas, va voir arsouyes.org
DNS .org
www.arsouyes.org ?
188.168.53.185
DNS arsouyes.org

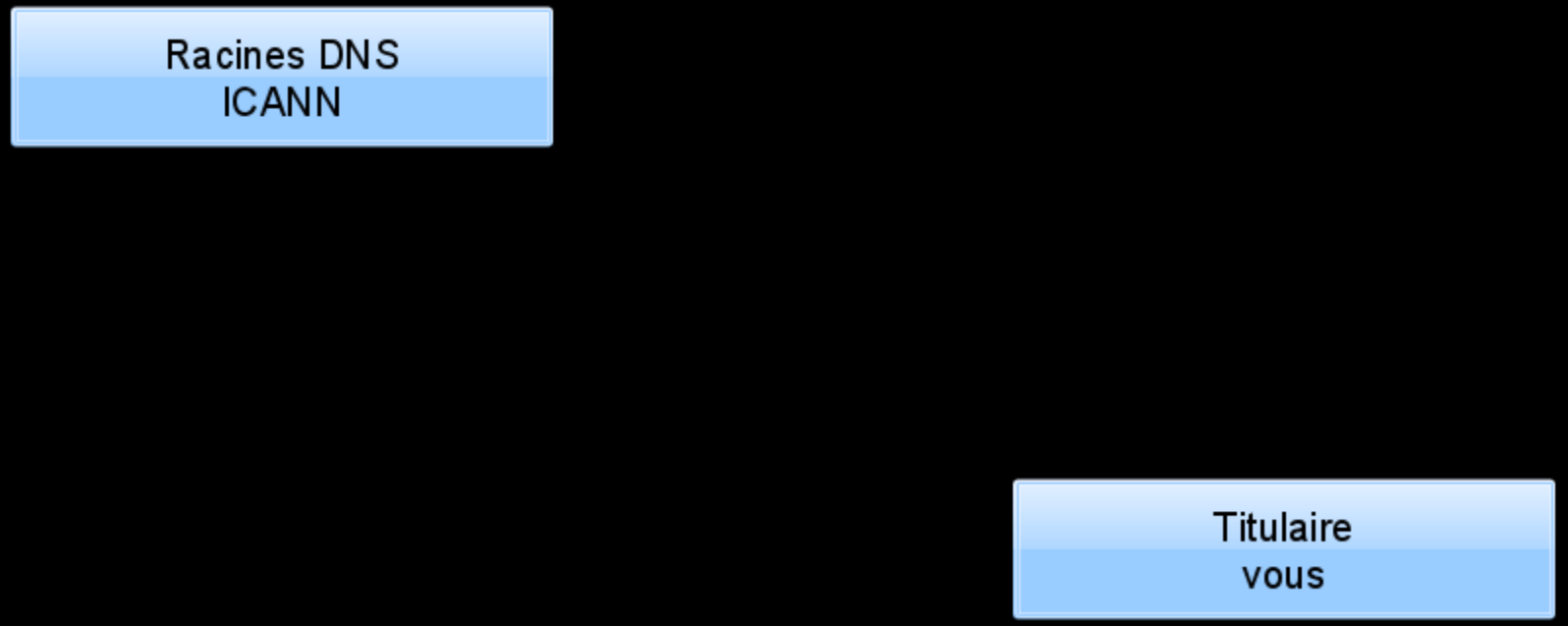
Requête DNS


Serveur DNS
Intermédiaire
Qui est "arsouyes.org" ?
C'est 188.168.53.185
www.arsouyes.org ?
Je sais pas, va voir .org
DNS Racine
www.arsouyes.org ?
Je sais pas, va voir arsouyes.org
DNS .org
www.arsouyes.org ?
188.168.53.185
DNS arsouyes.org

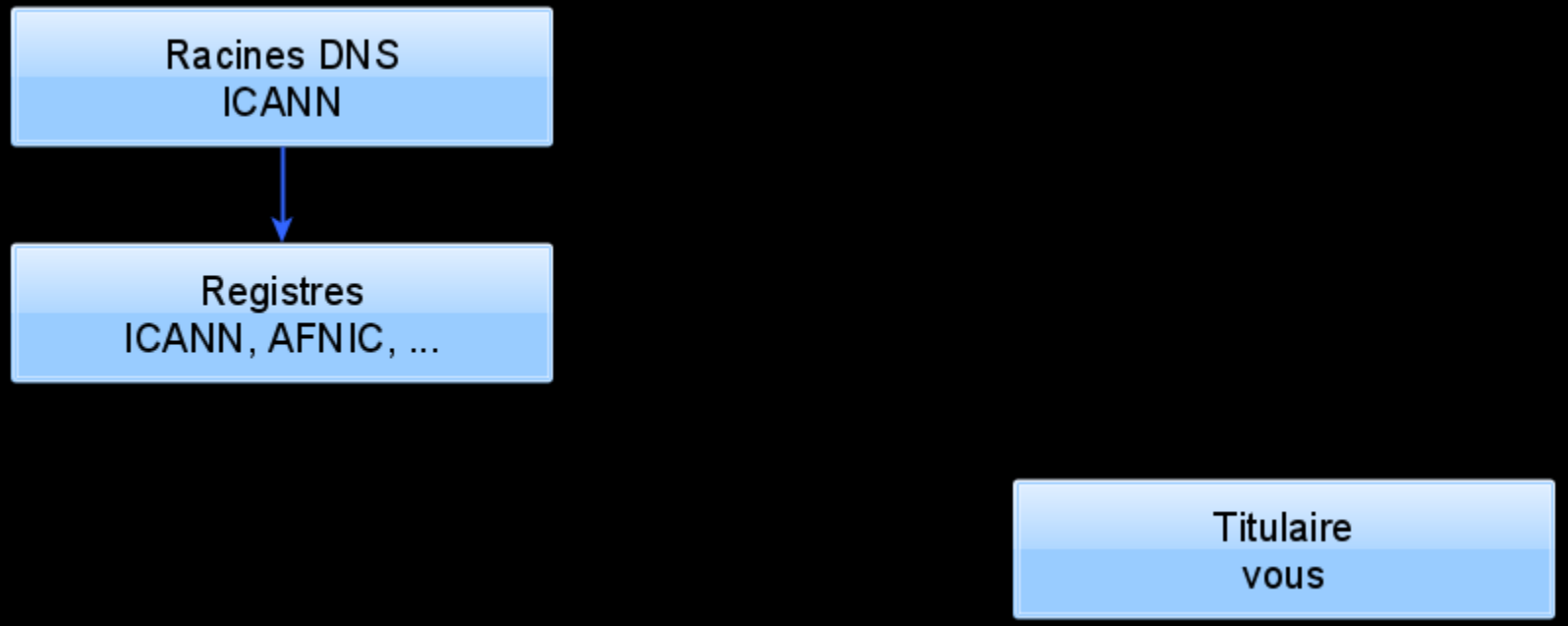
Principes d’organisation

Simple mais complexe aussi

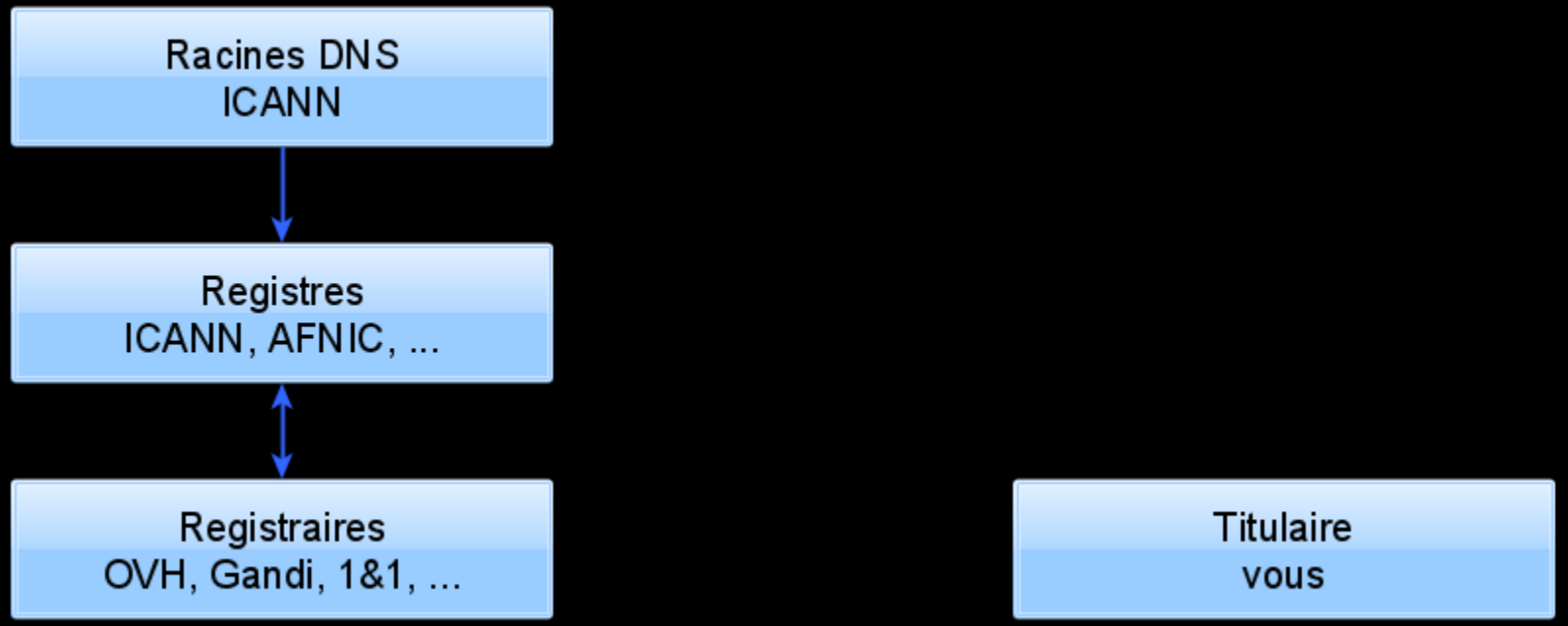
Organisation du DNS



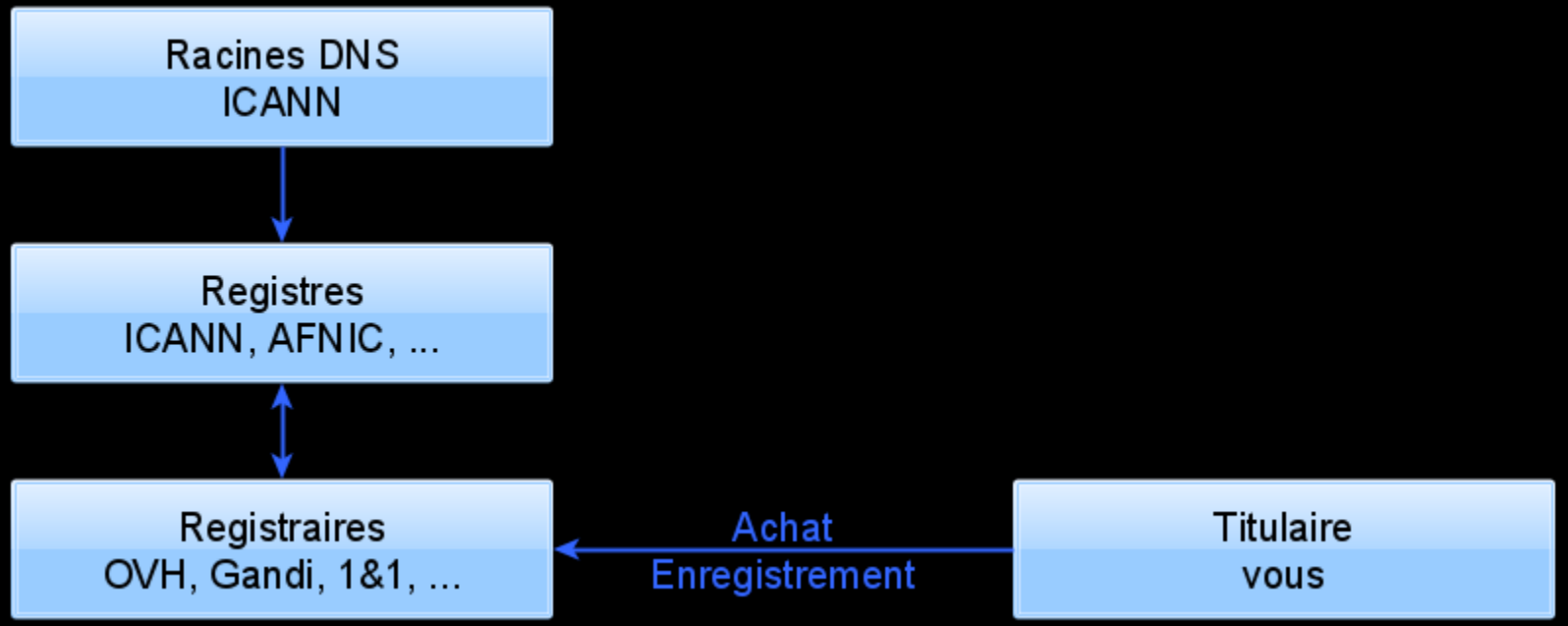
Organisation du DNS



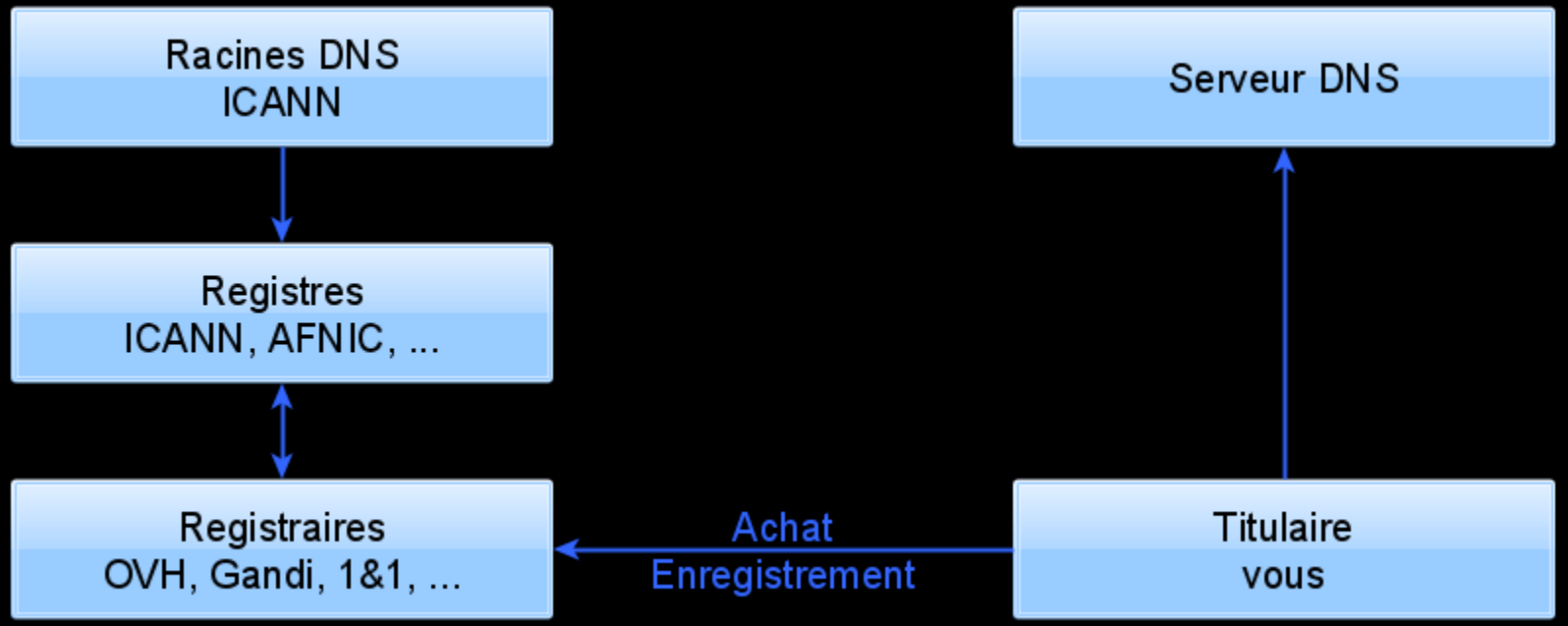
Organisation du DNS



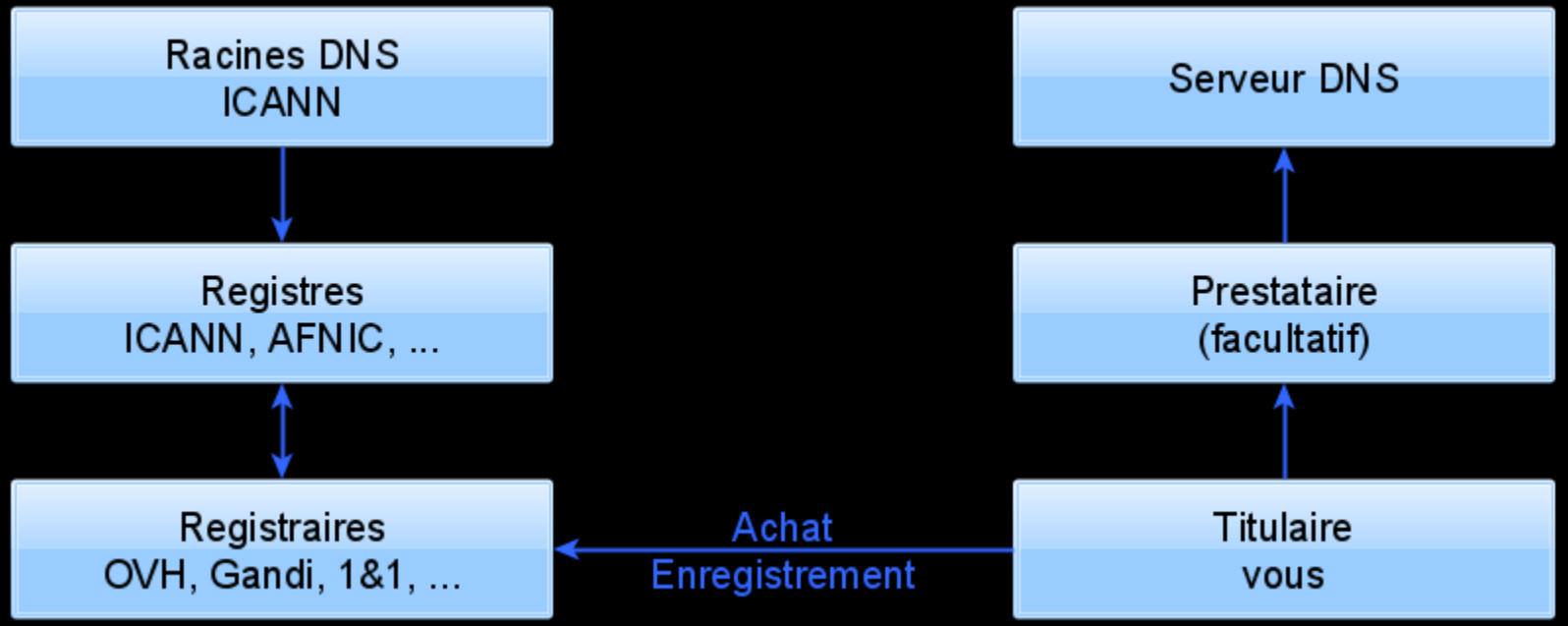
Organisation du DNS



Organisation du DNS



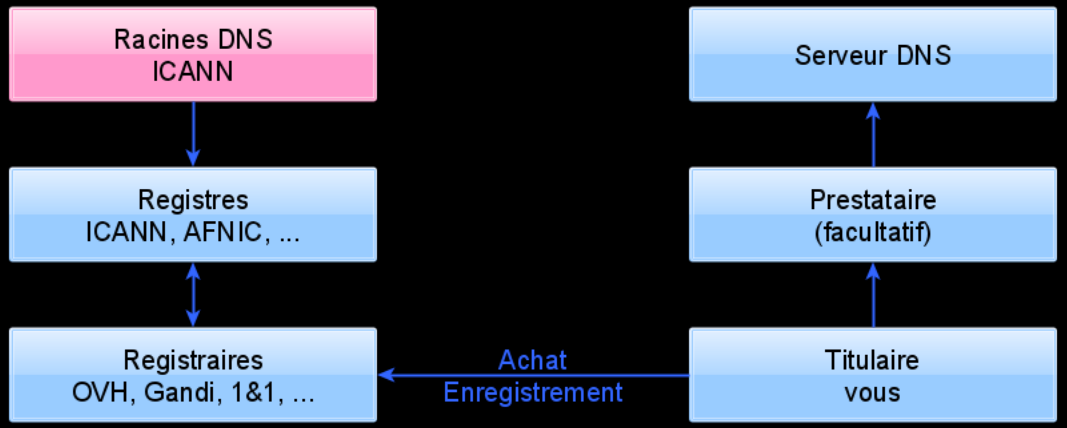
Organisation du DNS



Vulnérabilités des organisations

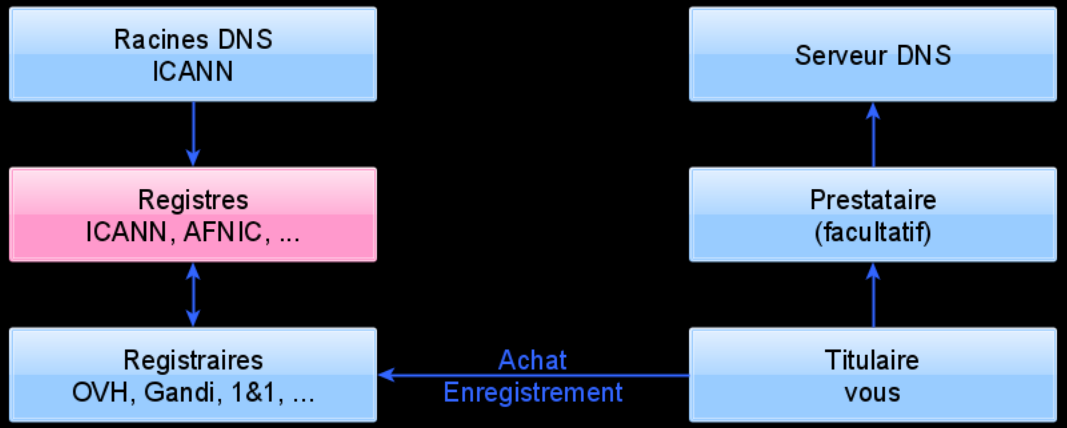
Pas besoin d’informatique

Vulnérabilités des racines



On n’y peut rien

Vulnérabilités des registres



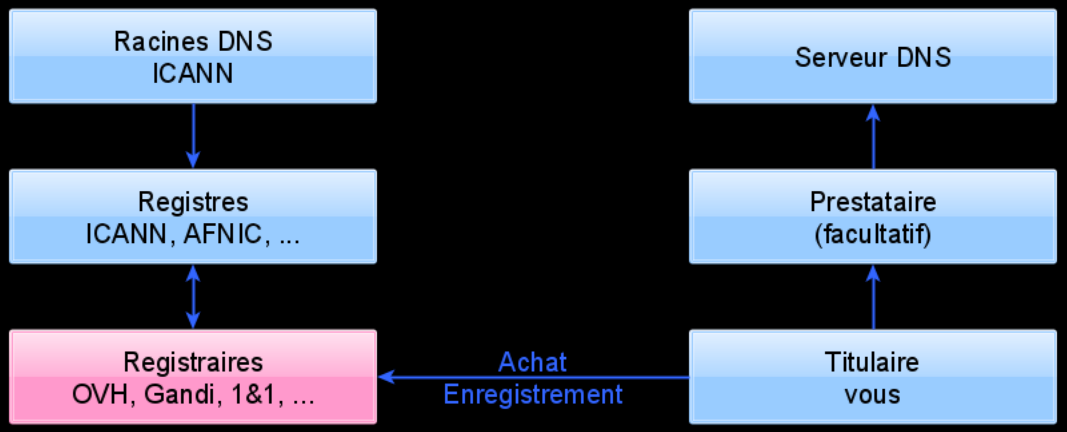
Choix du registre

.com *vs* .org *vs* .bzh

C’est déjà arrivé

e.g. EIDR en 2012

Vulnérabilités des registraires



« Verroux de registre »
(registre ou registraire)

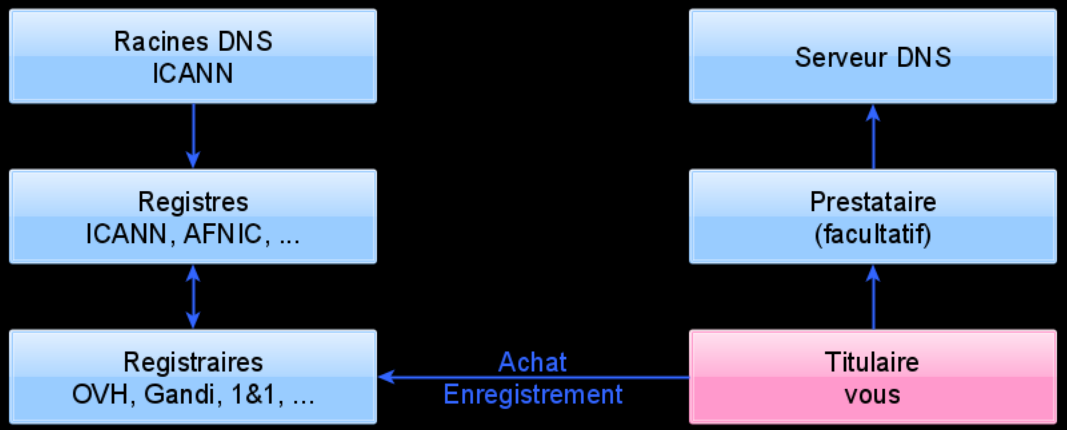
Ça arrive

2012 – godaddy

2013 - Network solution et NameCheap

2014 - Mark Monitor

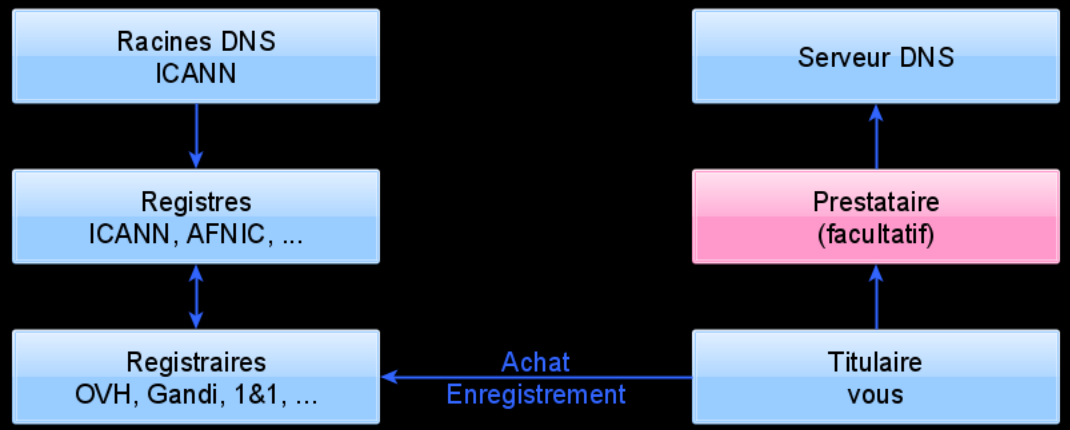
Vulnérabilités des propriétaires



Hygiène informatique

Verroux registraire

Vulnérabilités des prestataires

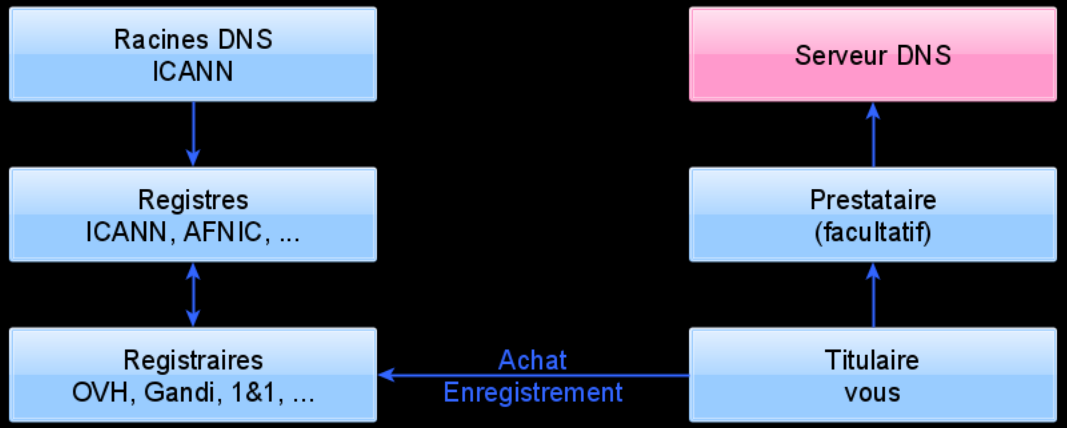


Choix du prestataire

Ça arrive

2013 – nytimes.com

Vulnérabilités des serveurs



Hygiène informatique

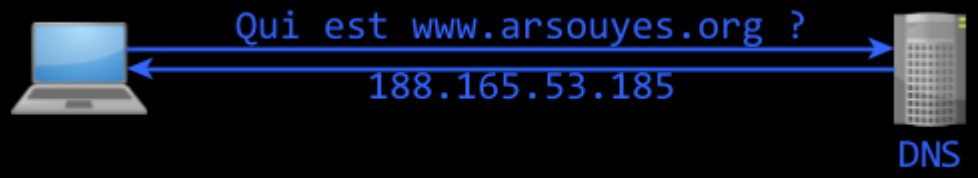
Guides de configurations

2004 – Spoofing

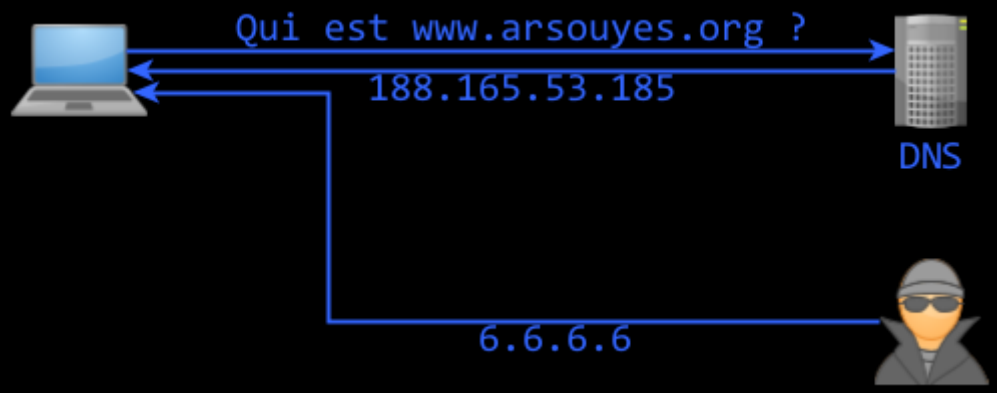
Phrack 62 – 0x03

Mistakes in the RFC Guidelines on DNS Spoofing Attacks

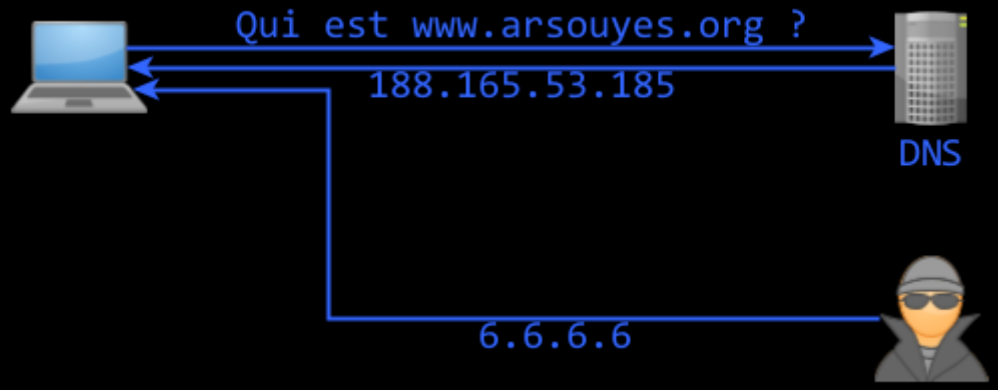
Requête DNS



Trop de réponses



Comment vérifier ?

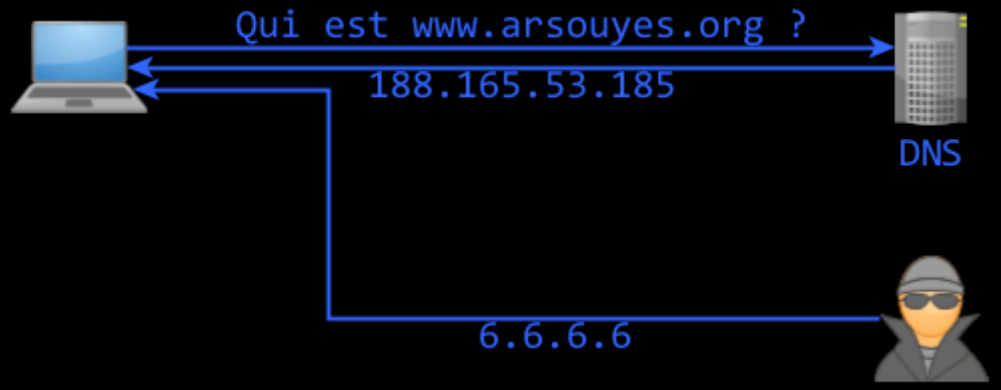


Nom de domaine

ID de transaction

N° de port UDP

Et en vrai ?



Nom de domaine

facultatif

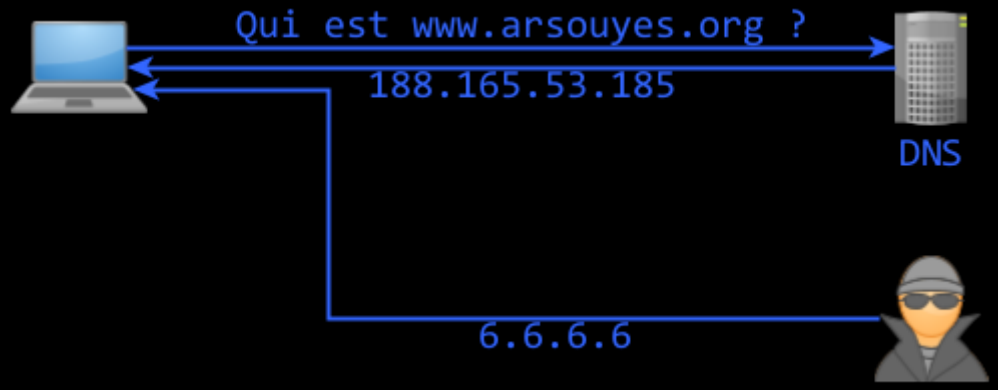
ID de transaction

1 puis Incrément

N° de port UDP

Constant (1026)

Solution



Nom de domaine

obligatoire

ID de transaction

Aléatoire : 16bits

N° de port UDP

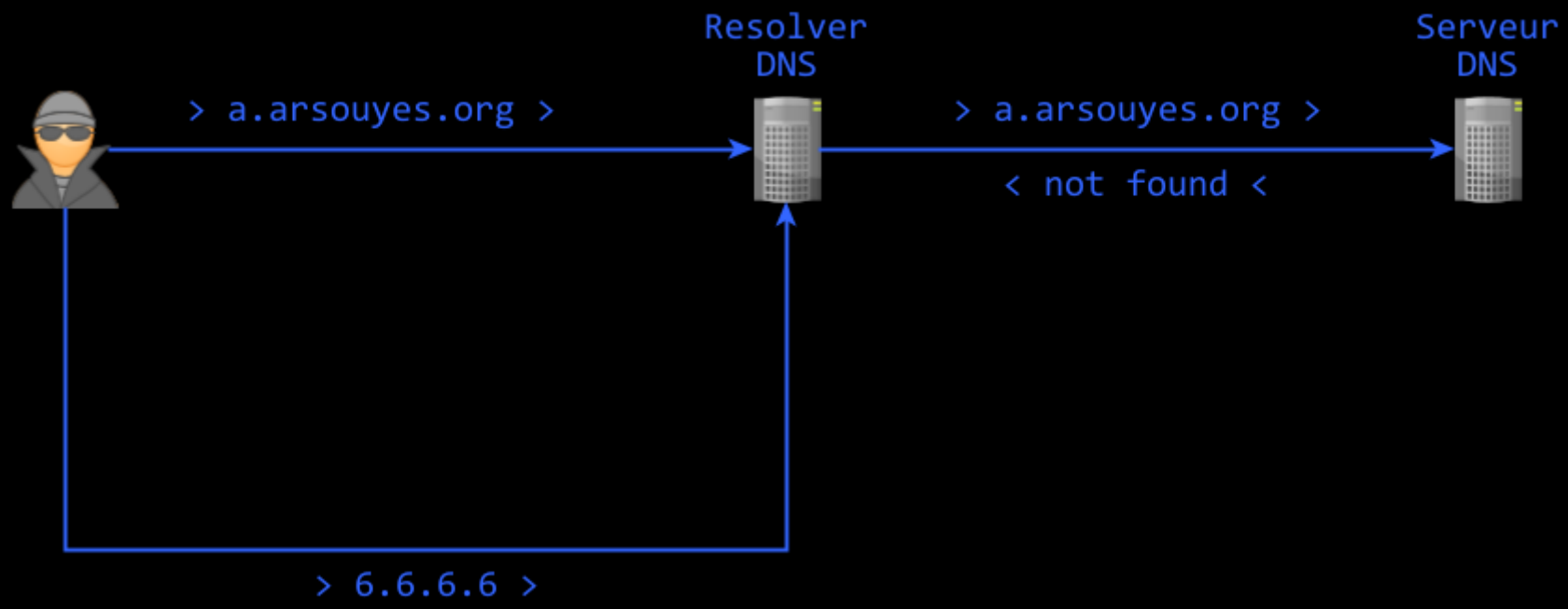
Aléatoire : 16 bits

2008 - Spoofing

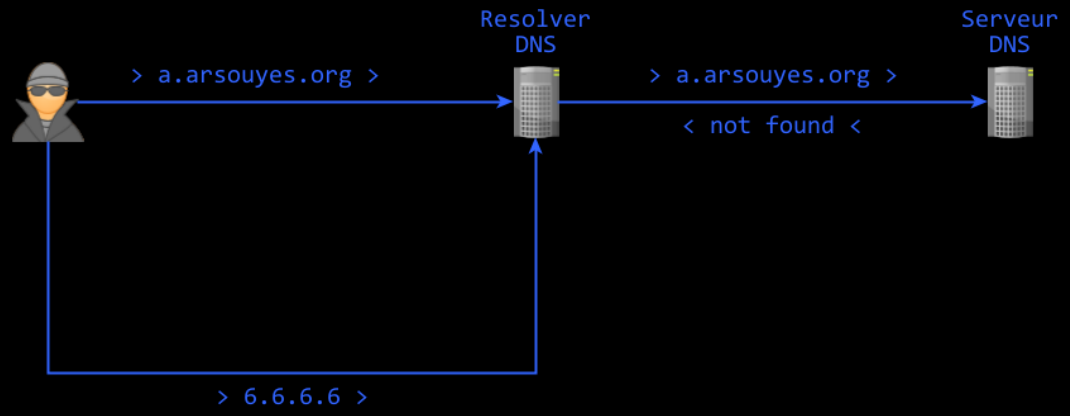
Dan Kaminski, Black Hat

DNS Intermédiaire

Spoofing sur l’intermédiaire



Parfois ça marche



Nom de domaine

Connu

Doit être « nouveau »

ID de transaction

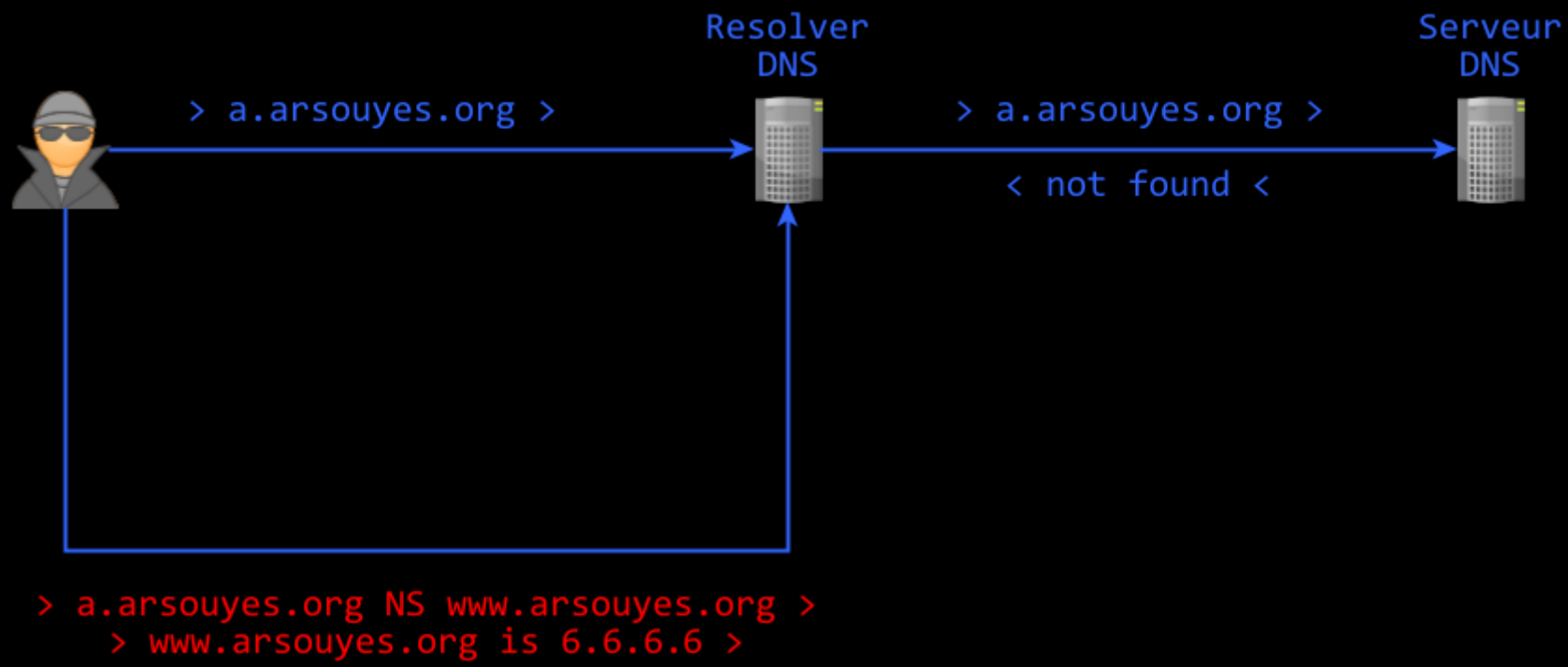
Aléatoire : 16bits

Parfois ça marche

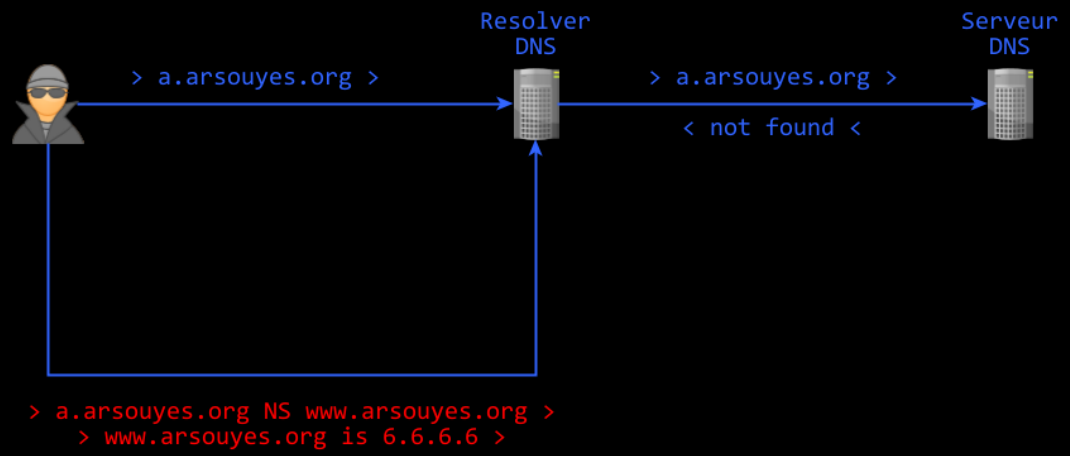
N° de port UDP

Constant

Fausse délégation + cache



Parfois ça marche



Nom de domaine

Arbitraire

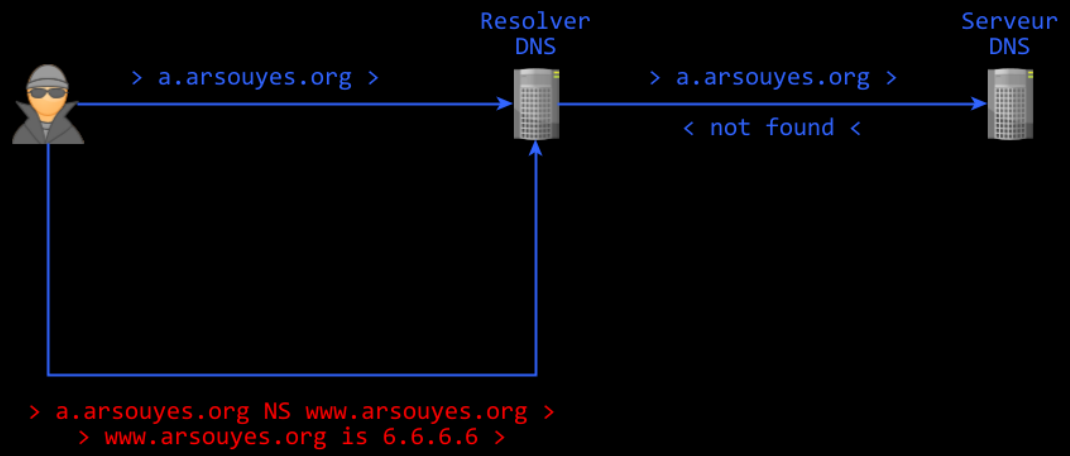
ID de transaction

A force, ça marche

N° de port UDP

Constant

Solution



Nom de domaine

Obligatoire

ID de transaction

Aléatoire

N° de port UDP

Aléatoire

2020 - Spoofing

Keyu Man & al.

Proceedings of ACM Conference on Computer and Communications Security

Exploiter en deux temps

N° de port

Réponse ICMP en cas d’erreur

ID de transaction

Comme en 2008

Solution Ultime

De la cryptographie…

DNSSEC

Depuis 1999

Déploie vraiment que depuis 2007/2009

Signature des enregistrements

Récursivement jusqu'aux racines

Pas toujours reconnus

Pfsense, freebox, redbox (sfr), sosh (orange), bouygues

sigok.verteiltesysteme.net – sigfail.verteilsysteme.net