Attaques et sécurisation des couches OSI
Cartographie de réseau

Carlos Aguilar
carlos.aguilar-melchor@isae-supaero.fr
Benoît Morgan
benoit.morgan@enseeiht.fr

IRIT

Remerciements

Merci à :

- Carlos Aguilar-Melchor
- Marc ”van Hauser” Heuse
- Cédric Blancher (EADS)
- Dan Boneh de Stanford University
- Pierre-François Bonnefoi du Master CRYPTIS à Limoges
- Céline Boyer (Canal+)
- Julien Cartigny du Master CRYPTIS à Limoges
- Ron Rivest du M.I.T.

Sources

[1] https://www.gnu.org/philosophy/free-sw.html
[2] https://tools.ietf.org/html/rfc3912
[3] https://tools.ietf.org/html/rfc1034

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Dans le cadre de la sécurité

Action de cartographier un réseau dans le but d'exécuter des interactions malveillantes avec ses systèmes.

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Dans le cadre de la sécurité

Action de cartographier un réseau dans le but d'exécuter des interactions malveillantes avec ses systèmes.

Pourquoi ?

- *For fun and profit* : *black-hats*

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Dans le cadre de la sécurité

Action de cartographier un réseau dans le but d'exécuter des interactions malveillantes avec ses systèmes.

Pourquoi ?

- *For fun and profit* : *black-hats*
- Pour évaluer la robustesse d'un réseau : *red teams* vs. *blue teams*

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Dans le cadre de la sécurité

Action de cartographier un réseau dans le but d'exécuter des interactions malveillantes avec ses systèmes.

Pourquoi ?

- *For fun and profit* : *black-hats*
- Pour évaluer la robustesse d'un réseau : *red teams* vs. *blue teams*
- Pour *monitorer* le réseau dans une optique de maintenance

Cartographie de réseau

S'il existait une définition générale

Action de constituer une base de connaissance sur les équipements et les hôtes d'un réseau, afin de construire un graphe d'interconnexions et d'accessibilités de services le plus précis possible.

Dans le cadre de la sécurité

Action de cartographier un réseau dans le but d'exécuter des interactions malveillantes avec ses systèmes.

Pourquoi ?

- *For fun and profit* : *black-hats*
- Pour évaluer la robustesse d'un réseau : *red teams* vs. *blue teams*
- Pour *monitorer* le réseau dans une optique de maintenance
- L'administrateur est parti à la retraite avec les plans :)

Tests d'intrusions : cibles et points d'entrée

Cible locale

- Un pied dans l'infrastructure de l'entité à évaluer...
- mais pas forcément sur le même domaine de diffusion
- Wi-Fi : portail captif, VLAN interne
- Ethernet cablé sur le réseau d'entreprise
- Réseau mobile

Tests d'intrusions : cibles et points d'entrée

Cible locale

- Un pied dans l'infrastructure de l'entité à évaluer...
- mais pas forcément sur le même domaine de diffusion
- Wi-Fi : portail captif, VLAN interne
- Ethernet cablé sur le réseau d'entreprise
- Réseau mobile

Cible distante

- À l'extérieur
- Connecté d'un façon ou d'un autre aux Internets...
- et par conséquent à notre cible

Méthode générale de test d'intrusion à distance

Recueil des informations

- Informations publiques sur l'entité
- Informations "actives" (protocoles réseau)

Méthode générale de test d'intrusion à distance

Recueil des informations

- Informations publiques sur l'entité
- Informations "actives" (protocoles réseau)

Cartographie du réseau

- Découverte des membres
- Découverte de la structure

Méthode générale de test d'intrusion à distance

Recueil des informations

- Informations publiques sur l'entité
- Informations "actives" (protocoles réseau)

Cartographie du réseau

- Découverte des membres
- Découverte de la structure

Évaluation (attaque)

- Mots de passes faibles
- Exploitation de vulnérabilités / mauvaises configurations connues

Méthode générale de test d'intrusion à distance

Recueil des informations

- Informations publiques sur l'entité
- Informations "actives" (protocoles réseau)

Cartographie du réseau

- Découverte des membres
- Découverte de la structure

Évaluation (attaque)

- Mots de passes faibles
- Exploitation de vulnérabilités / mauvaises configurations connues

Maintient de l'accès

- Portes dérobées
- Écoute du réseau

Méthode générale de test d'intrusion local

Identifier la cible

- On est déjà sur place !

Cartographie du réseau

- Idem

Évaluation

- Idem

Types de données par couche du modèle OSI 1/2

2 : couche liaison de données

- Information : hôtes connectés sur le domaine de diffusion local
- Adressage unique des machines (802.3, 802.11)
- Protocoles spécifiques (*Spanning Tree Protocol*)

Types de données par couche du modèle OSI 1/2

2 : couche liaison de données

- Information : hôtes connectés sur le domaine de diffusion local
- Adressage unique des machines (802.3, 802.11)
- Protocoles spécifiques (*Spanning Tree Protocol*)

3 : couche réseau

- Information : routeurs interconnectés formants des réseaux
- Adressage Internet
- Protocoles spécifiques (*IGP, EGP, ICMP*)

Types de données par couche du modèle OSI 1/2

2 : couche liaison de données

- Information : hôtes connectés sur le domaine de diffusion local
- Adressage unique des machines (802.3, 802.11)
- Protocoles spécifiques (*Spanning Tree Protocol*)

3 : couche réseau

- Information : routeurs interconnectés formants des réseaux
- Adressage Internet
- Protocoles spécifiques (*IGP, EGP, ICMP*)

4 : couche transport

- Information : services transportés et disponibles
- Adressage de services (ports)
- Protocoles spécifiques (*TCP, UDP*)

Types de données par couche du modèle OSI 2/2

7 : application

- Résolution de noms de domaines : DNS
- Résolution inverse d'adresse Internet : DNS
- Consultation des données administratives d'allocation d'adresses
- Consultation des données administratives d'allocation de nom de domaine

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Découverte des membres

Objectifs

- Étape préliminaire à l'évaluation
- Réseau local ou distant

Découverte des membres

Objectifs

- Étape préliminaire à l'évaluation
- Réseau local ou distant

Étapes

1. Découverte des hôtes du réseau
2. Découverte des services qu'ils proposent

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Découverte des hôtes

Objectifs

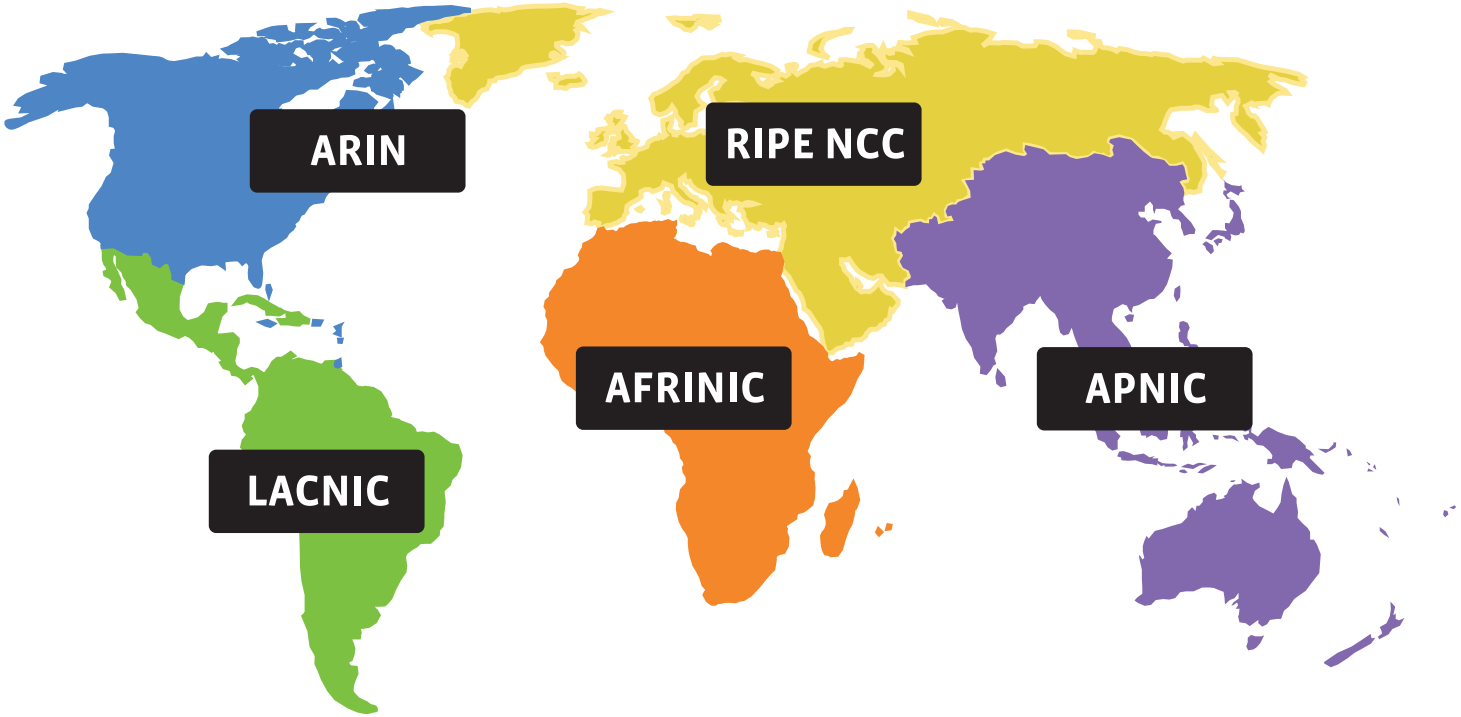
- Étape préliminaire à l'évaluation
- Données d'entrée : informations recueillies sur la cible
- Données de sortie : liste des hôtes du réseau

Méthode

- Interaction active
  - Couche réseau
  - Couche application (DNS / whois)
- Écoute passive
- Difficultés
  - Filtrage
  - IPv6

Adressage IP

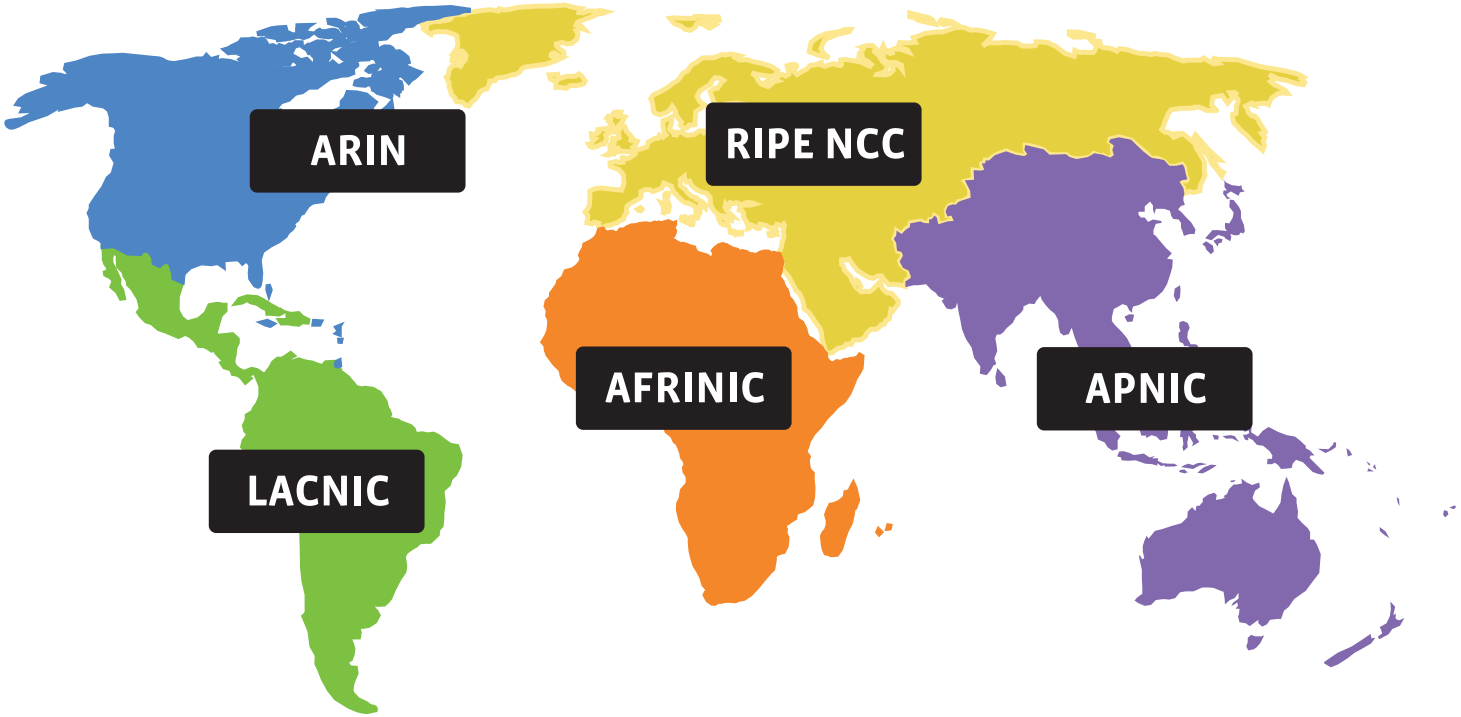
Responsabilités administratives



Adressage IP

Responsabilités administratives

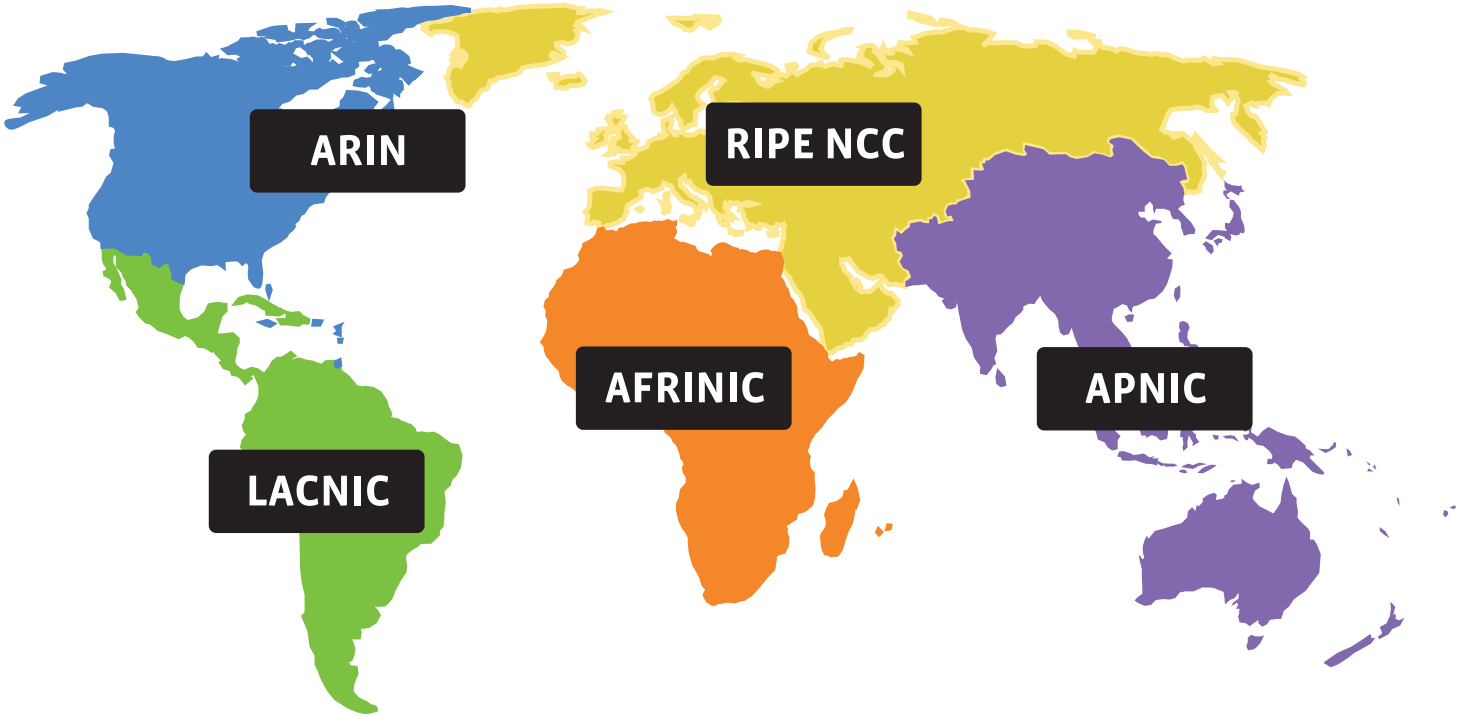
- ICANN



Adressage IP

Responsabilités administratives

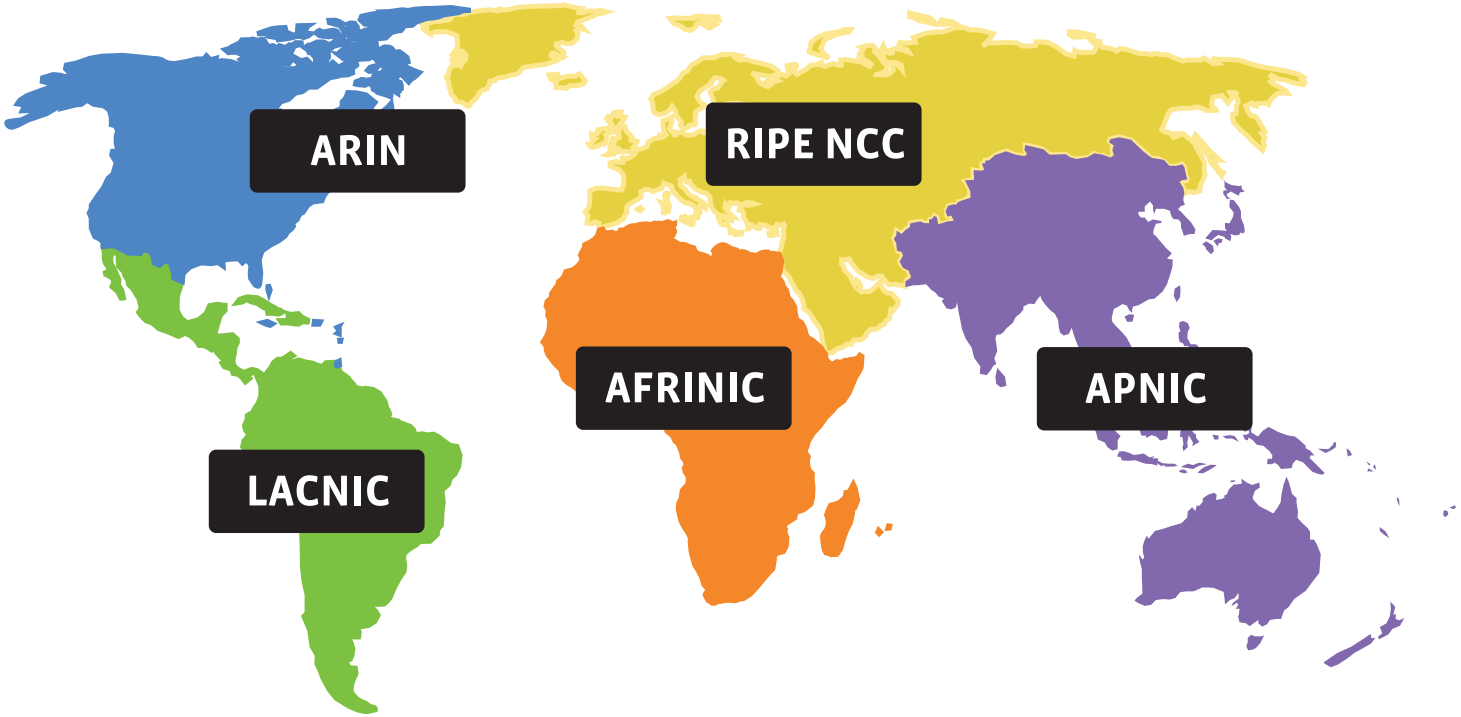
- ICANN → IANA



Adressage IP

Responsabilités administratives

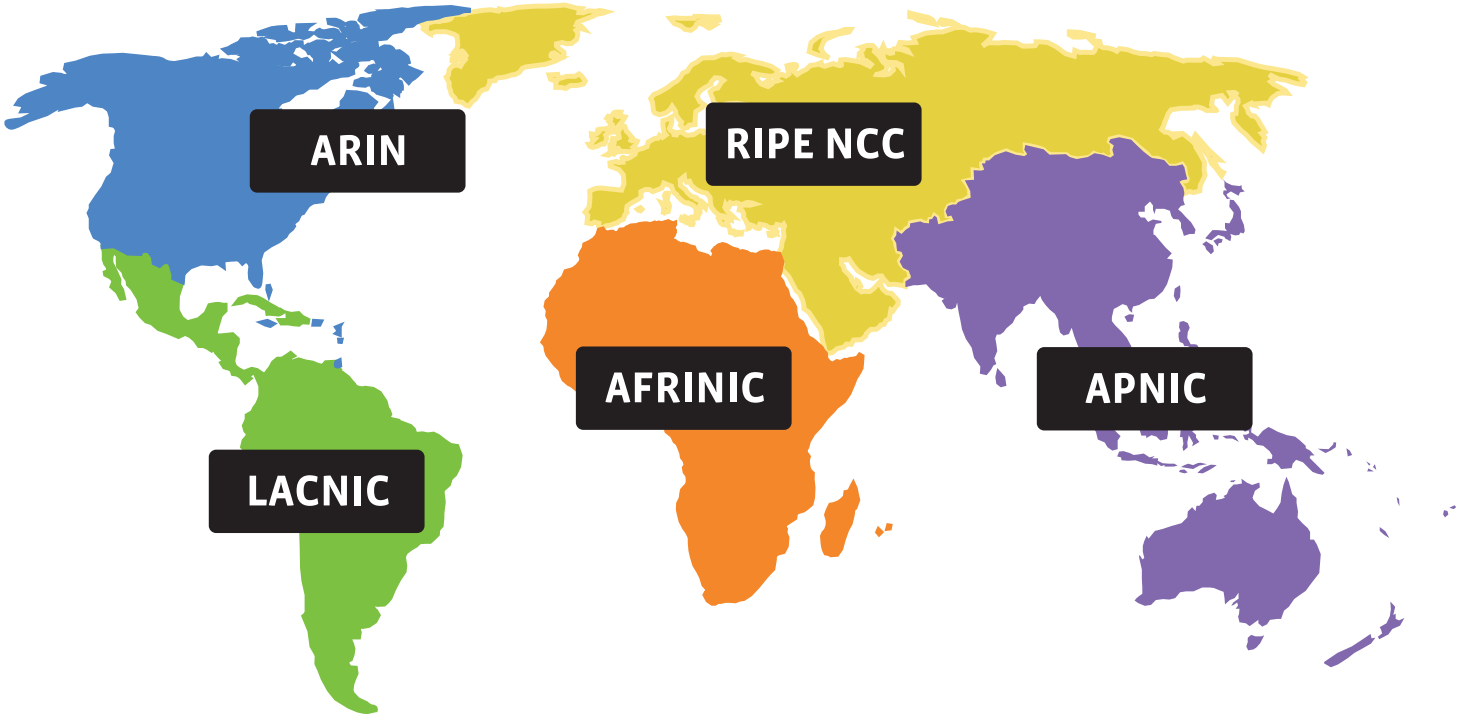
- ICANN → IANA → Regional Internet Registries (RIR)



Adressage IP

Responsabilités administratives

- ICANN → IANA → Regional Internet Registries (RIR)
- RIPE NCC, ARIN, etc.



Adressage IP

Allocation de plages d'adresses

- *For free (as in "free beer" this time)* [1]
- IANA : `net/8` → RIR
- RIR/LIR/ISP : nets → entities

⇒ Lien entre localité physique et réseau IP

Données publiques IANA

```
Prefix                    Designation                          Date
000/8  IANA - Local Identification                             1981-09
001/8  APNIC                                                   2010-01
002/8  RIPE NCC                                                2009-09
003/8  Administered by ARIN                                    1994-05
004/8  Level 3 Parent, LLC                                     1992-12
005/8  RIPE NCC                                                2010-11
006/8  Army Information Systems Center                         1994-02
007/8  Administered by ARIN                                    1995-04
[...]
```

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

Adressage IP

Responsible organisation: Orange S.A.
Abuse contact info: gestionip.ft@orange.com

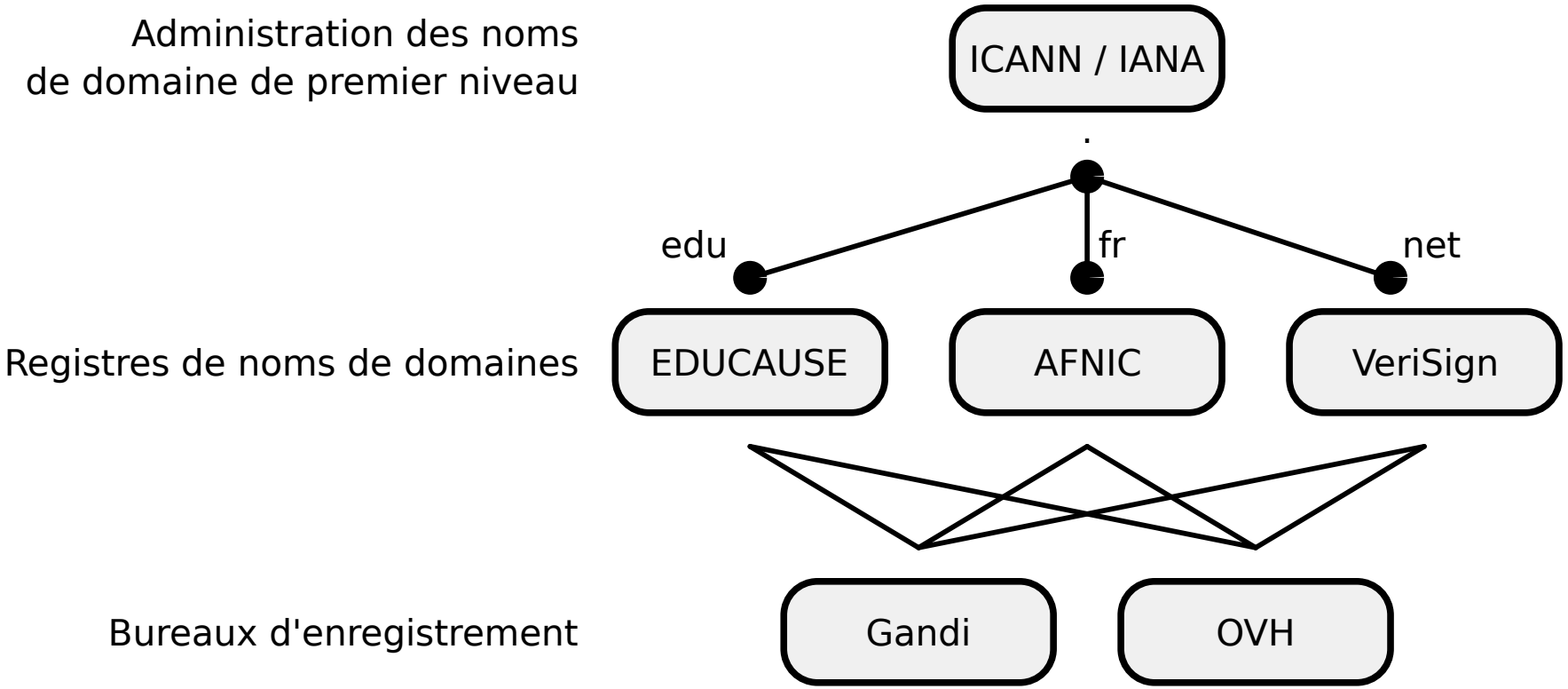
Login to update | RIPEstat

```
inetnum:        2.0.0.0 - 2.0.0.255
netname:        IP2000-ADSL-BAS
descr:          BSNAN651 Nantes Bloc 1
country:        FR
admin-c:        WITR1-RIPE
tech-c:         WITR1-RIPE
status:         ASSIGNED PA
remarks:        for hacking, spamming or security problems send mail to
remarks:        abuse@orange.fr
mnt-by:         FT-BRX
created:        2011-01-19T09:55:44Z
last-modified:  2011-07-05T13:48:25Z
source:         RIPE
```

https://apps.db.ripe.net/db-web-ui

Allocation de noms de domaines

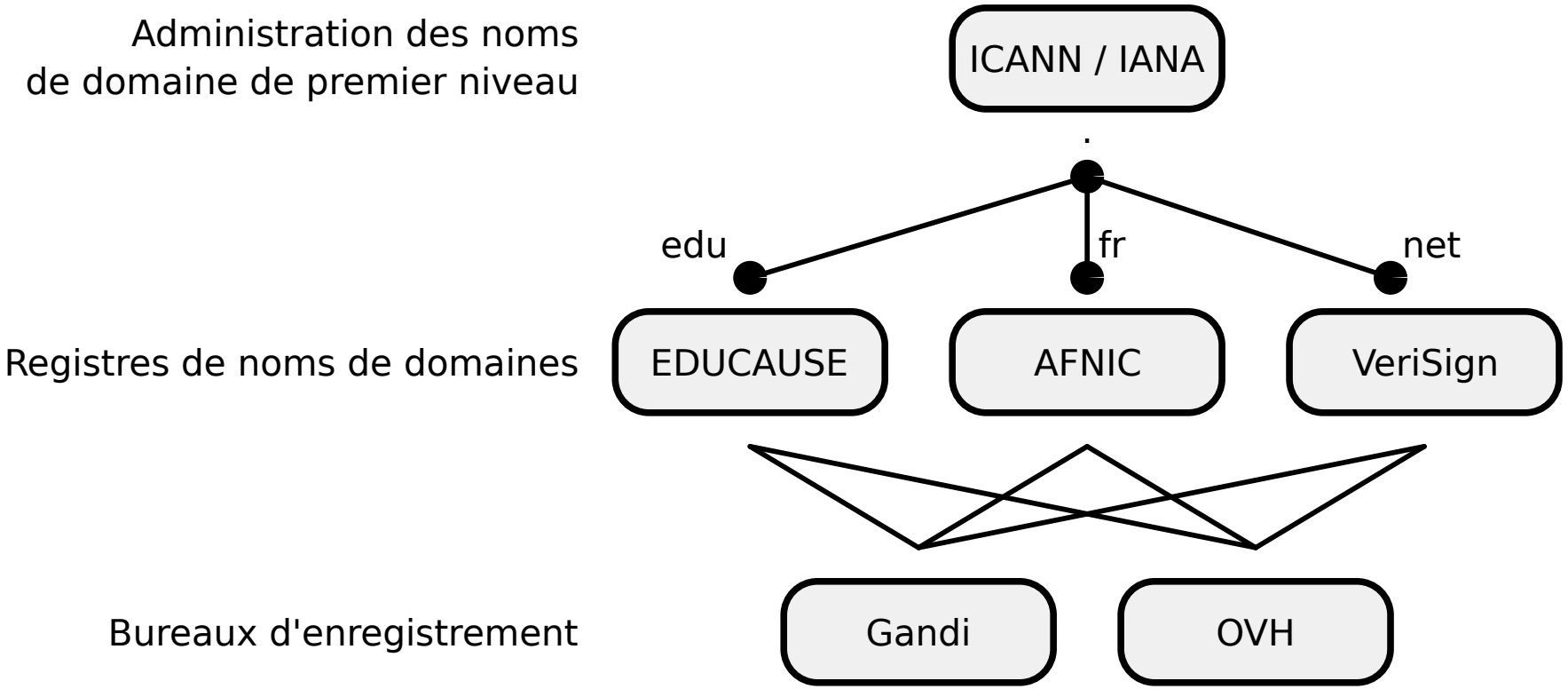
Responsabilités administratives



Allocation de noms de domaines

Responsabilités administratives

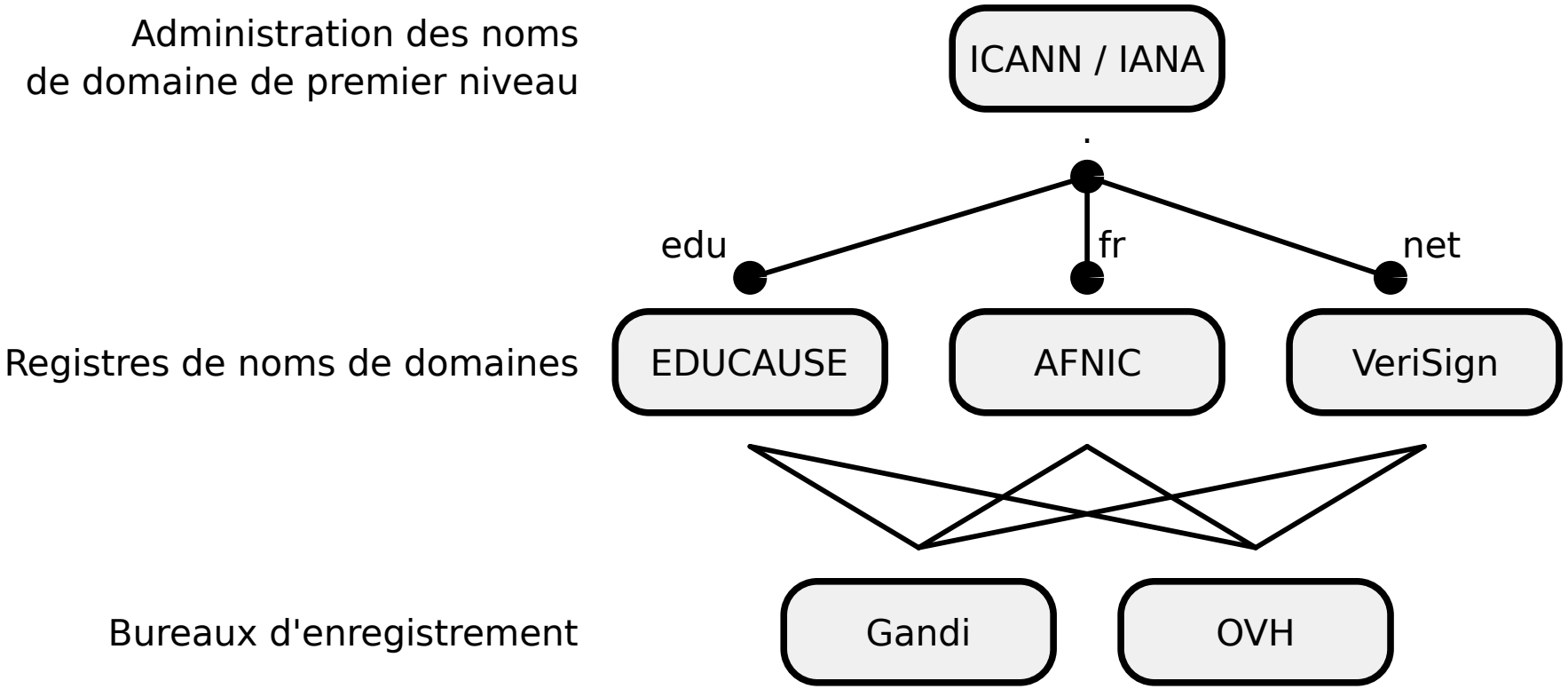
- ICANN



Allocation de noms de domaines

Responsabilités administratives

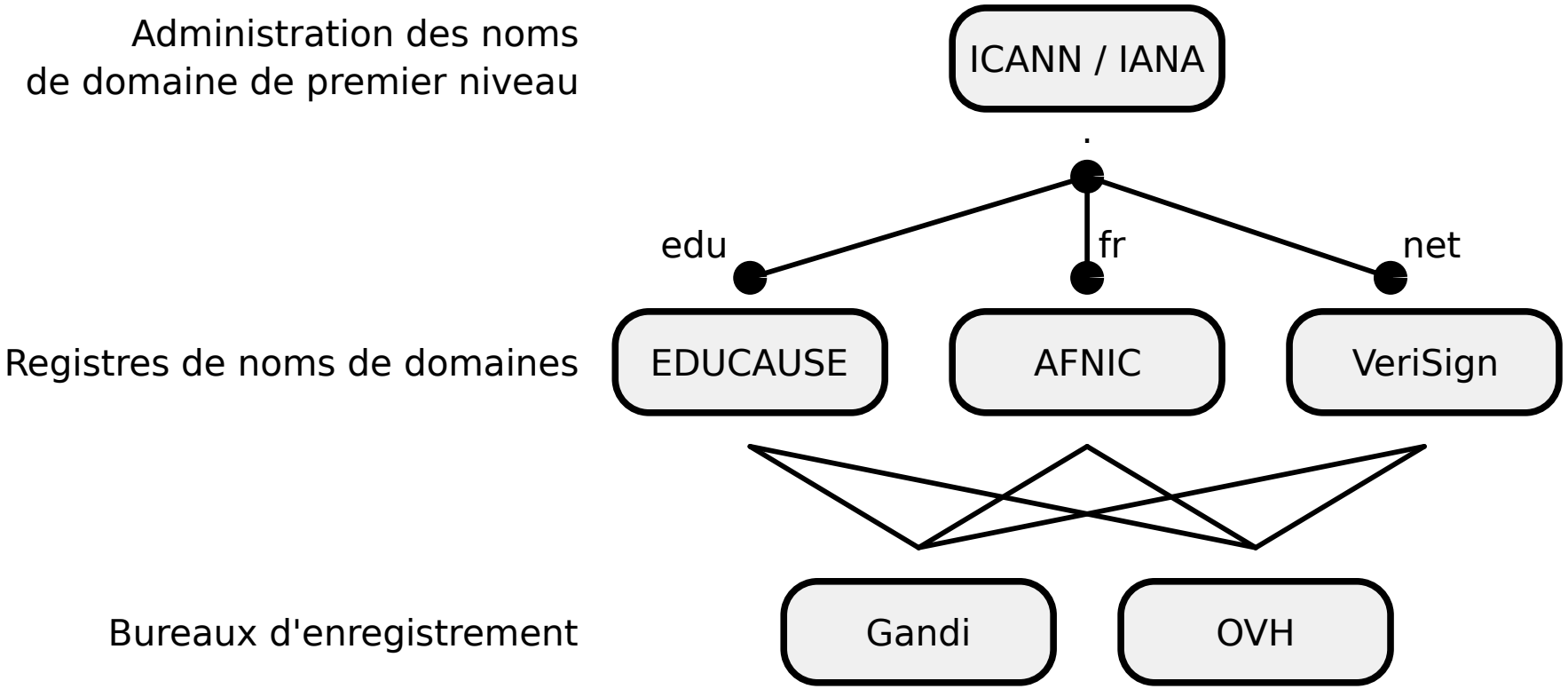
- ICANN → IANA



Allocation de noms de domaines

Responsabilités administratives

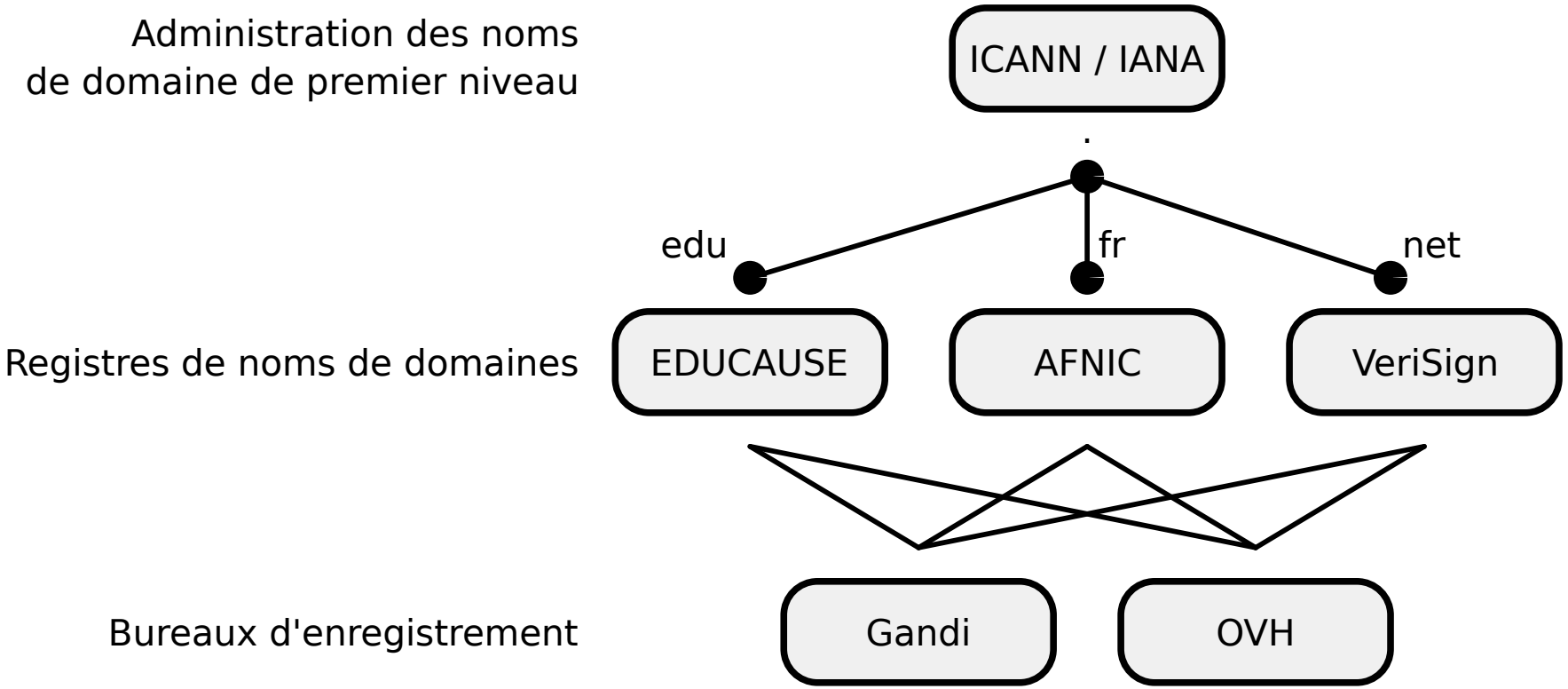
- ICANN → IANA → Registres de noms de domaines



Allocation de noms de domaines

Responsabilités administratives

- ICANN → IANA → Registres de noms de domaines → Bureaux d'enregistrements



Allocation de noms de domaines

Enregistrement

- Auprès d'un bureau d'enregistrement (OVH, Gandi, 1&1)
- Enregistrement gratuite
- Frais de dossier et hébergement de zone payants

⇒ Possible lien entre localité physique et nom de domaine

Allocation de noms de domaines

Données publiques des *NIC* : AFNIC pour `fr`.

Résultat de votre recherche

- **Nom de domaine :** enseeiht.fr
- **État :** Actif (consulter aussi le **site web**)
- **DNSSEC :** inactif
- **Bureau d'enregistrement :** **GIP RENATER**
- **Date de création :** 1 janvier 1995 00:00
- **Date d'expiration :** 1 janvier 2019 00:00
- **Serveurs de noms (DNS)**
  - ***Serveur n° 1:*** *ns1.enseeiht.fr*
  - ***Serveur n° 2:*** *ns2.nic.fr*
  - ***Serveur n° 3:*** *sivuca.leei.enseeiht.fr*

⊞ **Titulaire :** **INSTITUT NATIONAL POLYTECHNIQUE**

⊞ **Contact administratif :** **Alain Ayache**

⊞ **Contact technique :** **GIP RENATER**

⊞ **Contact technique :** **Jean-Claude Darcos**

⊞ **Contact technique :** **Brigitte Sor**

`https://www.afnic.fr/fr/produits-et-services/services/whois/`

Serveurs Whois

Service

- Protocole d'accès aux bases de données
- Des NIC et des bureaux d'enregistrement
- Des registres internet régionaux (RIR)

Serveurs Whois

Service

- Protocole d'accès aux bases de données
- Des NIC et des bureaux d'enregistrement
- Des registres internet régionaux (RIR)

Protocole

- Texte, TCP : 43
- RFC 3912 [2]
- Question réponse basique

Serveurs Whois

Service

- Protocole d'accès aux bases de données
- Des NIC et des bureaux d'enregistrement
- Des registres internet régionaux (RIR)

Protocole

- Texte, TCP : 43
- RFC 3912 [2]
- Question réponse basique

Objectifs

- "Standardisation" de l'accès aux bases de données

⇒ Outils de vérification de disponibilité DNS / IP

⇒ Bien pratique dans notes cas (cible)

Serveurs Whois

AFNIC

- `nc whois.afnic.fr 43`
- `enseeiht.fr`
- Soyez rapide ou pipe !

Serveurs Whois

AFNIC

- `nc whois.afnic.fr 43`
- `enseeiht.fr`
- Soyez rapide ou pipe !

RIPE NCC

- `nc whois.ripe.net 43`
- `193.48.203.0/24`

Serveurs Whois

AFNIC

- `nc whois.afnic.fr 43`
- `enseeiht.fr`
- Soyez rapide ou pipe !

RIPE NCC

- `nc whois.ripe.net 43`
- `193.48.203.0/24`

RIPE NCC

- `nc whois.ripe.net 43`
- `AS2200`

Programme whois

Problématique

- Quel serveur utiliser pour tel `/8` ?
- Quel serveur utiliser pour tel domaine de premier niveau ?

⇒ Uniformiser le point d'entrée aux services Whois

Programme whois

Problématique

- Quel serveur utiliser pour tel `/8` ?
- Quel serveur utiliser pour tel domaine de premier niveau ?

⇒ Uniformiser le point d'entrée aux services Whois

Solution

- Utilisation d'heuristiques servant à aiguiller l'utilisateur vers le bon serveur
- `man 1 whois`
- Quelles options peuvent nous intéresser ?

Whois : cartographie ?

Recueil d'information

- Obtenir des noms de personnes
- Obtenir des adresses mail

Whois : cartographie ?

Recueil d'information

- Obtenir des noms de personnes
- Obtenir des adresses mail

Découverte des membres

- Obtenir les noms des DNS

Programme whois

Exercice

- `$ whois enseeiht.fr`
- `$ whois 193.48.203.34`
- `$ whois AS2200`

DNS : serveur DNS d'autorité d'une entité

Stratégie locale

- Consultation du fichier `/etc/resolv.conf` d'une machine
- Écoute du traffic réseau local
  - Requêtes DNS
  - Dialogue DHCP

Stratégie distante

- INPI et assimilé → noms et termes
- Moteurs de recherche → hôtes
- Registre whois → DNS d'autorité

Configuration DNS : `/etc/resolv.conf`

Informations

- `nameserver` : DNS utilisé par la machine locale
- `domain` : domaine local (ex : `enseeiht.fr`)
- `search` : domaines de recherche
  - Utilisation de nom courts
  - `albator` ⇔ `albator.enseeiht.fr`
- Intuition sur d'autres services (domaine LDAP)

Génération

- resolvconf.conf(5), resolvconf(8)
  - DHCP
  - VPN *endpoints*

Configuration DNS : /etc/resolv.conf

```
$ cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search laas.fr
nameserver 140.93.5.46
nameserver 195.83.132.132
$ dig -x 140.93.5.46 +short
dns.laas.fr.
$ dig -x 195.83.132.132 +short
ombre.laas.fr.
```

Configuration DNS : démo DHCP

- Essayer

DNS : Les transferts de zone

A quoi ça sert ?

DNS : Les transferts de zone

A quoi ça sert ?

- À quoi sert l'enregistrement **SOA** et ses données ?

DNS : Les transferts de zone

A quoi ça sert ?

- À quoi sert l'enregistrement **SOA** et ses données ?
- Protocole de synchronisation entre serveurs maîtres et esclaves
- Exigence de la RFC 1034 [3].

DNS : Les transferts de zone

A quoi ça sert ?

- À quoi sert l'enregistrement **SOA** et ses données ?
- Protocole de synchronisation entre serveurs maîtres et esclaves
- Exigence de la RFC 1034 [3].

Protocole DNS

- Drapeaux : requête standard
- Drapeaux : non récursive
- Question : nom de zone à transférer
- Question : type axfr (`0x00fc`)

```
▸ Flags: 0x0020 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
▾ Queries
  ▸ enseeiht.fr: type AXFR, class IN
```

DNS : Les transferts de zone

Exercice

- Découvrir les serveurs DNS de l'N7
- Tenter de transférer des zones
- `$ dig @<serveur> <domaine> axfr`

DNS : Les transferts de zone

Serveurs DNS de l'N7

DNS : Les transferts de zone

Serveurs DNS de l'N7

```
$ dig enseeiht.fr +trace +all +additional
[...]
;; AUTHORITY SECTION:
enseeiht.fr.        172800  IN  NS  ns1.enseeiht.fr.
enseeiht.fr.        172800  IN  NS  sivuca.leei.enseeiht.fr.
enseeiht.fr.        172800  IN  NS  ns2.nic.fr.
[...]
;; ADDITIONAL SECTION:
ns1.enseeiht.fr.    172800  IN  A   147.127.176.22
ns2.nic.fr.     172800  IN  A   192.93.0.4
sivuca.leei.enseeiht.fr. 172800 IN  A   147.127.16.11
ns2.nic.fr.     172800  IN  AAAA    2001:660:3005:1::1:2
[...]
;; Query time: 103 msec
;; SERVER: 194.0.36.1#53(194.0.36.1)
;; WHEN: ven. oct. 26 11:56:52 CEST 2018
;; MSG SIZE  rcvd: 673
```

DNS : Les transferts de zone

Serveur `ns2.nic.fr`

DNS : Les transferts de zone

Serveur `ns2.nic.fr`

```
$ dig @192.93.0.4 enseeiht.fr axfr

; <<>> DiG 9.13.3 <<>> @192.93.0.4 enseeiht.fr axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

DNS : Les transferts de zone

Serveur `ns1.enseeiht.fr`

DNS : Les transferts de zone

Serveur `ns1.enseeiht.fr`

```
$ dig @147.127.176.22 enseeiht.fr axfr

; <<>> DiG 9.13.3 <<>> @147.127.176.22 enseeiht.fr axfr
; (1 server found)
;; global options: +cmd
[...]
albator.enseeiht.fr.    86400   IN  A   147.127.133.133
albatros.enseeiht.fr.   86400   IN  A   147.127.33.81
[...]
laserf102.enseeiht.fr.  86400   IN  A   147.127.33.85
laserf105.enseeiht.fr.  86400   IN  A   147.127.33.177
laserf111.enseeiht.fr.  86400   IN  A   147.127.33.38
laserf114.enseeiht.fr.  86400   IN  A   147.127.33.184
laserf115.enseeiht.fr.  86400   IN  A   147.127.33.14
laserf117.enseeiht.fr.  86400   IN  A   147.127.33.146
laserf118.enseeiht.fr.  86400   IN  A   147.127.33.118
laserf119.enseeiht.fr.  86400   IN  A   147.127.33.70
laserf121.enseeiht.fr.  86400   IN  A   147.127.33.62
[...]
```

Ça marche (idem pour `sivuca.leei.enseeiht.fr`)

DNS : Les transferts de zone

Informations

- Tous les enregistrements **A**, **AAAA**, **NS**, **CNAME**, **SOA** et **MX** en une seule reqête !
- Obtention d'une grande partie des membres du réseau (module les **CNAMES** et non nommés)

DNS : Les transferts de zone

Informations

- Tous les enregistrements **A**, **AAAA**, **NS**, **CNAME**, **SOA** et **MX** en une seule reqête !
- Obtention d'une grande partie des membres du réseau (module les **CNAMES** et non nommés)

⇒ Ressource critique !

DNS : Les transferts de zone

Informations

- Tous les enregistrements **A**, **AAAA**, **NS**, **CNAME**, **SOA** et **MX** en une seule reqête !
- Obtention d'une grande partie des membres du réseau (module les **CNAMES** et non nommés)

⇒ Ressource critique !

Sécurité

- Accessible que depuis les serveurs esclaves

DNS : Les transferts de zone

Informations

- Tous les enregistrements **A**, **AAAA**, **NS**, **CNAME**, **SOA** et **MX** en une seule reqête !
- Obtention d'une grande partie des membres du réseau (module les **CNAMES** et non nommés)

⇒ Ressource critique !

Sécurité

- Accessible que depuis les serveurs esclaves
- Et le parent de délégation

DNS : Les transferts de zone sans `axfr`

Exercice : utilisation d'un script et de résolution inversée

DNS : Les transferts de zone sans axfr

Exercice : utilisation d'un script et de résolution inversée

```
#!/bin/bash
for i in `seq 0 255`
do
  for j in `seq 0 255`
  do
    ip="193.48.$i.$j"; echo -n "$ip -> "; res=`dig -x $ip +short`; echo $res
  done
done
```

DNS : Les transferts de zone sans `axfr`

Exercice : utilisation d'un script et de résolution inversée

```
#!/bin/bash
for i in `seq 0 255`
do
  for j in `seq 0 255`
  do
    ip="193.48.$i.$j"; echo -n "$ip -> "; res=`dig -x $ip +short`; echo $res
  done
done
```

Sortie

```
193.48.203.0 ->
193.48.203.1 -> gw-dmz.inp-toulouse.fr.
193.48.203.2 ->
[...]
193.48.203.193 -> fc-193.inp-toulouse.fr.
193.48.203.194 -> fc-194.inp-toulouse.fr.
193.48.203.195 -> fc-195.inp-toulouse.fr.
193.48.203.255 ->
[...]
```

DNS : Les transferts de zone sans `axfr`

Exercice : utilisation d'un script et de résolution inversée

```
#!/bin/bash
for i in `seq 0 255`
do
  for j in `seq 0 255`
  do
    ip="193.48.$i.$j"; echo -n "$ip -> "; res=`dig -x $ip +short`; echo $res
  done
done
```

Sortie

```
193.48.203.0 ->
193.48.203.1 -> gw-dmz.inp-toulouse.fr.
193.48.203.2 ->
[...]
193.48.203.193 -> fc-193.inp-toulouse.fr.
193.48.203.194 -> fc-194.inp-toulouse.fr.
193.48.203.195 -> fc-195.inp-toulouse.fr.
193.48.203.255 ->
[...]
```

Équivalence ?

DNS : DNSSEC walking

Enregistrement DNSSEC **NSEC**

- Preuve de non existence d'enregistrement DNS
- Liste chaînée d'enregistrement **NSEC**
- Ordre canonique des noms de dommaines de la zone

DNS : DNSSEC walking

Enregistrement DNSSEC **NSEC**

- Preuve de non existence d'enregistrement DNS
- Liste chaînée d'enregistrement **NSEC**
- Ordre canonique des noms de dommaines de la zone
- Pointant vers le prochain nom existant

DNS : DNSSEC walking

Enregistrement DNSSEC **NSEC**

- Preuve de non existence d'enregistrement DNS
- Liste chaînée d'enregistrement **NSEC**
- Ordre canonique des noms de dommaines de la zone
- Pointant vers le prochain nom existant

Informations

- Liste la totalité des noms présents
- Et des enregistrements présents pour ces noms

DNS : DNSSEC walking

Enregistrement DNSSEC **NSEC**

- Preuve de non existence d'enregistrement DNS
- Liste chaînée d'enregistrement **NSEC**
- Ordre canonique des noms de dommaines de la zone
- Pointant vers le prochain nom existant

Informations

- Liste la totalité des noms présents
- Et des enregistrements présents pour ces noms

⇒ Chef, on vient de se tirer dans les pieds !

DNS : DNSSEC walking

Enregistrement DNSSEC **NSEC**

- Preuve de non existence d'enregistrement DNS
- Liste chaînée d'enregistrement **NSEC**
- Ordre canonique des noms de dommaines de la zone
- Pointant vers le prochain nom existant

Informations

- Liste la totalité des noms présents
- Et des enregistrements présents pour ces noms

⇒ Chef, on vient de se tirer dans les pieds !

Conséquences

- Parcours de enregistrements **NSEC** un par un.

⇒ Service équivalent au transfert de zone..

DNS : DNSSEC walking

Exercice

- Scripter un parcours de zone DNSSEC
- Tenter de parcourir la zone `'.'` des serveurs racines
- `dig @<serveur-racine> <zone> <enregistrement>`

DNS : DNSSEC walking

Soution

DNS : DNSSEC walking

Soution

```
#!/bin/bash
# should be res='.'
zone='art.'
res=$zone
while test -n $res
do
  res=`dig @m.root-servers.net. $res NSEC +short | awk '{print $1}'`
  echo $res
  dig +short NS $res
  # End of zone
  if test $res = $zone; then break; fi
  echo $res
done
```

DNS : DNSSEC walking

Soution

```
#!/bin/bash
# should be res='.'
zone='art.'
res=$zone
while test -n $res
do
  res=`dig @m.root-servers.net. $res NSEC +short | awk '{print $1}'`
  echo $res
  dig +short NS $res
  # End of zone
  if test $res = $zone; then break; fi
  echo $res
done
```

Sortie

```
[...]
arte.
as.
asda.
asia.
associates.
[...]
```

DNS : DNSSEC walking

Soution

```
#!/bin/bash
# should be res='.'
zone='art.'
res=$zone
while test -n $res
do
  res=`dig @m.root-servers.net. $res NSEC +short | awk '{print $1}'`
  echo $res
  dig +short NS $res
  # End of zone
  if test $res = $zone; then break; fi
  echo $res
done
```

Sortie

```
[...]
arte.
as.
asda.
asia.
associates.
[...]
```

Équivalence ?

Découverte des hôtes par balayage

Méthode

- Parcours de tout l'espace d'adressage IP d'un réseau
- Interaction active avec les hôtes potentiels

Découverte des hôtes par balayage

Méthode

- Parcours de tout l'espace d'adressage IP d'un réseau
- Interaction active avec les hôtes potentiels

Exercice

- Ecrire un script qui rend ce service
- Utilisation d'ICMP

Découverte des hôtes par balayage

Cible

```
$ dig svc.laas.fr +short
140.93.69.42
```

Découverte des hôtes par balayage

Cible

```
$ dig svc.laas.fr +short
140.93.69.42
```

Solution

```
#!/bin/bash
for i in `seq 0 255`
do
  echo 147.127.160.$i
  ping -4 -c 1 -W 1 147.127.160.$i | grep transmitted
done
```

Découverte des hôtes par balayage

Cible

```
$ dig svc.laas.fr +short
140.93.69.42
```

Solution

```
#!/bin/bash
for i in `seq 0 255`
do
  echo 147.127.160.$i
  ping -4 -c 1 -W 1 147.127.160.$i | grep transmitted
done
```

Sortie

```
[...]
1 packets transmitted, 1 received, 0% packet loss, time 0ms
140.93.69.43
1 packets transmitted, 0 received, 100% packet loss, time 0ms
140.93.69.44
1 packets transmitted, 1 received, 0% packet loss, time 0ms
140.93.69.45
[...]
```

Découverte des hôtes locaux par balayage

Méthode

- Parcours de tout l'espace d'adressage IP d'un réseau local
- Interaction active avec les hôtes potentiels

Découverte des hôtes locaux par balayage

Méthode

- Parcours de tout l'espace d'adressage IP d'un réseau local
- Interaction active avec les hôtes potentiels

Exercice

- Ecrire un script qui rend ce service
- Utilisation d'ARP avec scapy
- `$ sudo scapy`
- `srp(Ether(dst="<mac-dst>")/ARP(pdst=<addr-dst>))`

Découverte des hôtes par balayage

Solution

```
#!/usr/bin/env python

# from scapy.sendrecv import srp
# from scapy.layers.l2 import Ether, ARP, conf
# or
from scapy.all import *

hosts = []

for host in range(1, 255):
  # addr = "172.22.224.%d" % (host)
  addr = "147.127.92.%d" % (host)
  print("Scanning host %d..." % (host))
  arp = Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=addr)
  # ans, unans = srp(arp, timeout=1, verbose=False, iface="wlan0")
  ans, unans = srp(arp, timeout=1, verbose=False, iface="eth0")
  if len(ans) > 0:
    print("answer: %s:%s -> %s:%s" % (ans[0][1].hwsrc, ans[0][1].psrc,
      ans[0][1].hwdst, ans[0][1].pdst))
    hosts.append(addr)
  else:
    print("timeout....")

print("Hosts list %s" % (hosts))
```

Découverte des hôtes par balayage

Sortie

```
$ sudo ./scan-arp.py
Scanning host 1...
timeout....
[...]
Scanning host 76...
answer: a8:b8:6e:48:ba:27:192.168.1.76 -> 64:5d:86:cb:c3:fc:192.168.1.61
[...]
Scanning host 253...
timeout....
Scanning host 254...
answer: 6c:38:a1:4e:0e:84:192.168.1.254 -> 64:5d:86:cb:c3:fc:192.168.1.61
Hosts list ['192.168.1.76', '192.168.1.254']
```

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Découverte des services

Objectifs

- Étape préliminaire à l'évaluation
- Données d'entrée : les hôtes présents
- Données de sortie : liste de couples (hôte, service)

Méthode

- Interaction active
  - Couche transport
  - Numéro de services connus
- Inférence à l'aide des données collectées sur l'hôte
- Difficultés
  - Filtrage
  - Numéro de service non standard

Découverte des services par balayage

Méthode

- Parcours d'une partie de l'espace des numéros de service
- Interaction active avec l'hôte ciblé

Découverte des services par balayage

Méthode

- Parcours d'une partie de l'espace des numéros de service
- Interaction active avec l'hôte ciblé

Exercice

- Ecrire un script qui rend ce service
- Utilisation de TCP SYN avec scapy
- `$ sudo scapy`
- `sr1(IP(dst="<ip>")/TCP(dport=<port>,flags="<tcp-flags>"))`

Regardez ce qu'il se passe avec Wireshark !

Découverte des services par balayage

Solution

```
#!/usr/bin/env python

from scapy.sendrecv import sr1
from scapy.layers.inet import IP
from scapy.layers.inet import TCP

ports = []

for port in range(1, 60):
  addr = "193.48.203.34"
  print("Scanning port %d..." % (port))
  pkt = sr1(IP(dst=addr)/TCP(dport=port,flags="S"), timeout=1, verbose=False)
  if pkt != None:
    print("answer: %s:%d -> %s:%d" % (pkt.src, pkt.sport, pkt.dst, pkt.dport))
    if pkt['TCP'].flags == "SA":
      ports.append(port)
      print("SYN/ACK")
    else:
      print("This port seems closed")
  else:
    print("timeout....")

print("Open ports %s" % (ports))
```

Découverte des services par balayage

Sortie

```
$ sudo ./scan-tcp-syn.py
Scanning port 0...
answer: 89.234.156.200:0 -> 192.168.1.61:20
This port seems closed
[...]
Scanning port 22...
answer: 89.234.156.200:22 -> 192.168.1.61:20
SYN/ACK
[...]
Scanning port 80...
answer: 89.234.156.200:80 -> 192.168.1.61:20
SYN/ACK
[...]
Scanning port 99...
answer: 89.234.156.200:99 -> 192.168.1.61:20
This port seems closed
Open ports [22, 80]
```

Découverte des services par balayage

Sortie

```
$ sudo ./scan-tcp-syn.py
Scanning port 0...
answer: 89.234.156.200:0 -> 192.168.1.61:20
This port seems closed
[...]
Scanning port 22...
answer: 89.234.156.200:22 -> 192.168.1.61:20
SYN/ACK
[...]
Scanning port 80...
answer: 89.234.156.200:80 -> 192.168.1.61:20
SYN/ACK
[...]
Scanning port 99...
answer: 89.234.156.200:99 -> 192.168.1.61:20
This port seems closed
Open ports [22, 80]
```

En quoi la pile IP nous aide ?
Pourquoi ?

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

L'outil Nmap

Services

- Découverte des hôtes
- Découverte des services
- Découverte du système d'exploitation hôte

L'outil Nmap

Services

- Découverte des hôtes
- Découverte des services
- Découverte du système d'exploitation hôte

Principe

- Envoyer des paquets : ARP,ICMP (echo request, timestamp, netmask), TCP (SYN, ACK, Null, FIN), IP
- En suivant éventuellement des techniques pour éviter la détection (fragmentation, decoy cloak, IP/MAC spoofing, random payload, bogus checksum, ...)
- Puis analyser les réponses pour obtenir les informations demandées (up, protocoles, ports, SE)

L'outil Nmap

Définition des cibles

`nmap [options] setofHosts1 [setofHosts2 [...]]`

Les hôtes qui vont subir le scan peuvent être définis de plusieurs façons.
Exemple :

`nmap scanme.nmap.org 192.168.0.0/24 147.127.80,83-88.-`

Actions

Nmap réalise par défaut trois actions : découverte des hôtes (ping scan), puis sur les hôtes qui sont up, reverse-DNS et scan de ports communs TCP

`-A`	Faire aussi un traceroute et essayer de deviner le SE en se basant sur les services et les banners
`-PN`	Ne pas faire le ping scan et tenter les deux autres étapes sur tous les hôtes
`-p ports`	Définir un ou des ports à tester au lieu des ports classiques (ex : `nmap -p 22 cibles`)
`-n|-R`	Pas de reverse-DNS / reverse-DNS pour tous

Scan d'un réseau

Le *list scan*

`nmap -sL cibles`

Comportement le moins intrusif : reverse-DNS sur chaque cible et s'arrêter
→ on obtient les noms de domaine de chaque machine qui en a un :

- Donne des informations sur à quoi sert la machine (ex : `fw.irit.fr`)
- Ne révèle pas les machines up qui n'ont pas de nom de domaine
- Ne dit pas si une machine donnée est en ligne ou pas

Le *ping scan*

`nmap -sP cibles`

Deuxième comportement le moins intrusif : essayer de découvrir parmi les cibles lesquelles sont up puis s'arrêter
Comportement par défaut :

- Cible locale : bakayage ARP
- À distance : un ICMP echo request, un TCP SYN au port 443, un TCP ACK au port 80, et un ICMP timestamp par hôte

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Découverte de la structure

Objectifs

- Étape préliminaire à l'évaluation
- Réseau local ou distant
- Couche réseau ou liaison de données

Découverte de la structure

Objectifs

- Étape préliminaire à l'évaluation
- Réseau local ou distant
- Couche réseau ou liaison de données

Information principales

1. Découverte des routeurs d'interconnexion
2. Découverte de l'organisation des commutateurs

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

Découverte des routeurs

Méthode

- Interaction active avec les hôtes du réseau découverts

1. Sélection d'une cible d'un autre domaine de diffusion
2. Découvrir le nombre et l'identité des sauts sur le chemin
3. Passer à la cible suivante et revenir à l'étape 1

$\Rightarrow$ Construction du graphe d'interconnexion

Découverte des routeurs IP

Utilisation du *Time To Live* IP

- On envoie plusieurs paquets à la même cible
- On commence avec un TTL de 1 et on l'incrémente à chaque paquet

On regarde l'adresse IP des paquets ICMP *Time Exceeded* reçus

Découverte des routeurs IP

Utilisation du *Time To Live* IP

- On envoie plusieurs paquets à la même cible
- On commence avec un TTL de 1 et on l'incrémente à chaque paquet

On regarde l'adresse IP des paquets ICMP *Time Exceeded* reçus

Résultat attendu

- Le nombre de routeurs traversés
- La liste des adresses IP des routeurs

Découverte des routeurs IP

Exercice

- Ecrire un script qui rend ce service
- Utilisation d'ICMP *echo request* avec scapy
- `$ sudo scapy`
- `srp(IP(dst = "<IP-dst>", ttl = 1) / ICMP())`

Découverte des routeurs IP

Solution

```
#!/usr/bin/env python

from scapy.all import *

dst="172.217.19.35"

for i in range(1,255):
  replies, unans = sr(IP(dst = dst,ttl = i) / ICMP(), timeout = 1, verbose =
      False)
  if len(replies) == 1:
    a, b = replies[0]
    if b.type == 11 or b.type == 0:
      if (dst == b.src):
        print("Fin de la decouverte des routeurs %s" % b.src)
        exit()
      else:
        print("New routeur %s" % b.src)
  else:
    print("Timeout")
```

Découverte des routeurs IP

Sortie

```
$ sudo ./traceroute.py
New routeur 192.168.1.254
New routeur 10.171.152.2
New routeur 212.194.171.160
New routeur 212.194.171.137
Timeout
New routeur 72.14.213.208
Timeout
New routeur 216.239.43.98
New routeur 209.85.251.93
Fin de la découverte des routeurs 8.8.8.8
```

Programme `traceroute`

Service

- Découvre les routeurs traversés pour une communication
- Recherche DNS inverse des adresses IP des routeurs
- Supporte plusieurs charges utiles (ICMP *echo* ou TCP SYN)

traceroute à l'ENSEEIHT

```
$ traceroute ns1.enseeiht.fr
traceroute to ns1.enseeiht.fr (147.127.176.22), 30 hops max, 60 byte packets
1 147.127.80.200 (147.127.80.200) 1.246 ms 1.242 ms 1.518 ms
2 ns1.enseeiht.fr (147.127.176.22) 0.253 ms 0.260 ms 0.259 ms
```

```
$ traceroute google.fr
traceroute to google.fr (172.217.19.35), 30 hops max, 60 byte packets
 1  futunafw.enseeiht.fr (147.127.240.201)  0.313 ms  0.272 ms  0.251 ms
 2  fw80int1.enseeiht.fr (147.127.80.9)  0.439 ms  0.433 ms  0.418 ms
 3  172.22.130.17 (172.22.130.17)  1.261 ms  1.296 ms  1.308 ms
 4  193.55.105.98 (193.55.105.98)  3.196 ms  3.063 ms  3.202 ms
 5  * * *
 6  te2-3-montpellier-rtr-021.noc.renater.fr (193.51.177.224)  7.914 ms  8.009
      ms  7.987 ms
 7  xe1-0-3-marseille1-rtr-131.noc.renater.fr (193.51.177.18)  13.711 ms  8.613
       ms  8.569 ms
 8  te2-6-marseille2-rtr-021.noc.renater.fr (193.51.177.213)  8.501 ms te1-1-
      marseille2-rtr-021.noc.renater.fr (193.51.177.185)  8.504 ms te2-6-
      marseille2-rtr-021.noc.renater.fr (193.51.177.213)  8.440 ms
 9  72.14.218.132 (72.14.218.132)  8.417 ms  8.318 ms  8.360 ms
10  108.170.252.225 (108.170.252.225)  8.661 ms 108.170.252.241
     (108.170.252.241)  8.697 ms  8.539 ms
11  66.249.95.55 (66.249.95.55)  8.610 ms 72.14.233.67 (72.14.233.67)  8.594 ms
       8.598 ms
12  mrs08s03-in-f3.1e100.net (172.217.19.35)  7.844 ms  7.897 ms  7.845 ms
```

Plus d'informations sur la route ? 1/2

Quel réseau explorer ?

```
$ whois 193.55.105.99
[...]
inetnum: 193.55.105.0 - 193.55.105.255
netname: FR-REMIP2000
descr:   Metropolitan Network Toulouse City
country: FR
[...]
```

Plus d'informations sur la route ? 2/2

Autres adresses

Quelles sont les adresses de notre routeur ?

```
#!/usr/bin/env python
from scapy.sendrecv import sr
from scapy.layers.inet import IP, ICMP
addrs = []
for i in range(1,255):
  # On fait augementer le TTL entre deux scan pour détecter les sous réseaux
  # routés par le ou les routeurs accessibles avec le TTL de base
  replies, unans = sr(IP(dst = "193.55.105.%s" % i, ttl = 5) / ICMP(), timeout
      = 0.1)
  if len(replies) == 1:
    a, b = replies[0]
    if b.type == 0:
      addrs.append("193.55.105.%s" % i)
print(addrs)
```

Plus d'informations sur la route ? 2/2

Autres adresses

Quelles sont les adresses de notre routeur ?

```
#!/usr/bin/env python
from scapy.sendrecv import sr
from scapy.layers.inet import IP, ICMP
addrs = []
for i in range(1,255):
  # On fait augementer le TTL entre deux scan pour détecter les sous réseaux
  # routés par le ou les routeurs accessibles avec le TTL de base
  replies, unans = sr(IP(dst = "193.55.105.%s" % i, ttl = 5) / ICMP(), timeout
      = 0.1)
  if len(replies) == 1:
    a, b = replies[0]
    if b.type == 0:
      addrs.append("193.55.105.%s" % i)
print(addrs)
```

TTL = 4 → '193.55.105.1', '193.55.105.2', '193.55.105.9', '193.55.105.10', ...

Plus d'informations sur la route ? 2/2

Autres adresses

Quelles sont les adresses de notre routeur ?

```
#!/usr/bin/env python
from scapy.sendrecv import sr
from scapy.layers.inet import IP, ICMP
addrs = []
for i in range(1,255):
  # On fait augementer le TTL entre deux scan pour détecter les sous réseaux
  # routés par le ou les routeurs accessibles avec le TTL de base
  replies, unans = sr(IP(dst = "193.55.105.%s" % i, ttl = 5) / ICMP(), timeout
      = 0.1)
  if len(replies) == 1:
    a, b = replies[0]
    if b.type == 0:
      addrs.append("193.55.105.%s" % i)
print(addrs)
```

TTL = 4 → '193.55.105.1', '193.55.105.2', '193.55.105.9', '193.55.105.10', ...

TTL = 5 → '193.55.105.1', '193.55.105.2', '193.55.105.3', '193.55.105.4', ...

Plus d'informations sur la route ? 2/2

Autres adresses

Quelles sont les adresses de notre routeur ?

```
#!/usr/bin/env python
from scapy.sendrecv import sr
from scapy.layers.inet import IP, ICMP
addrs = []
for i in range(1,255):
  # On fait augementer le TTL entre deux scan pour détecter les sous réseaux
  # routés par le ou les routeurs accessibles avec le TTL de base
  replies, unans = sr(IP(dst = "193.55.105.%s" % i, ttl = 5) / ICMP(), timeout
      = 0.1)
  if len(replies) == 1:
    a, b = replies[0]
    if b.type == 0:
      addrs.append("193.55.105.%s" % i)
print(addrs)
```

TTL = 4 → '193.55.105.1', '193.55.105.2', '193.55.105.9', '193.55.105.10', ...

TTL = 5 → '193.55.105.1', '193.55.105.2', '193.55.105.3', '193.55.105.4', ...

La différence des deux listes met en avant d'autres sous réseaux

Plan

1. Introduction
   - Objectifs et concepts
2. Découverte des membres
   - Découverte des hôtes
   - Découverte de services
   - Outils pour la découverte des membres
3. Découverte de la structure
   - Couche réseau
   - Couche liaison de données
4. Conclusion

ARP/CDP/STP/PVST+

Qui fait des requêtes ARP ?

Autres membres du réseau, et le(s) routeur(s) juste au-dessus de nous

Qui fait du STP ?

Le commutateur au dessus de nous

Problèmes de compatibilité

Certains commutateurs utilisent des versions améliorées (PVST+)
... que d'autres ne comprennent pas et relayent ! $\rightarrow$ commutateurs à un ou deux sauts

Contremesures

Configurer le matériel pour qu'il ne diffuse ces informations que sur les liens entre commutateurs
Et écouter ce qui circule dans le réseau !

Fin

Fin