ZADYREE M_101 KMKZ

Crawling into your ISP

Explore the world with one click =D

Disclaimer

- All the following stuff was done by professionals. Do not try it at home.
- Because of pressure, we cannot disclose the full content of what we discovered.

The beginning

- Dangerous hackers ? No, just hobbysts !

- M_101 : Forensic Student, app. Fan’
- Zadyree : Pentester, app. killer
- Kmkz : Network student, explorer

Agenda

- Do we really need an army to own a country ?
- Network Mapping
- Exploitation ?
- Aftermatch
- Questions ?

Do we really need an army to own a country ?

- Starting point : Hotspot bypassing
- The importance of an ISP and its security policy
- Security problems ?

Network Mapping

First surprise (ADSL routers) :

```
Host 172.xx.x.1 appears to be up.
Host 172.xx.x.65 appears to be up.
Host 172.xx.x.169 appears to be up.
Host 172.xx.x.193 appears to be up.
Host 172.xx.x.249 appears to be up.
```

Second surprise (VOIP servers) :

```
All 1715 scanned ports on 172.xx.xx.33
OS guesses: Microsoft Windows Server 2003 SP1 (96%)
```

Network Mapping

Third surprise (DNS servers)

```
Host 80.xx.xx.193 appears to be up.
Host 80.xx.xx.195 appears to be up.

Host 80.xx.xx.207 appears to be up.
```

And gateway to cisco routers (ETH0 80.X.X.X / ETH1 172.X.X.X)

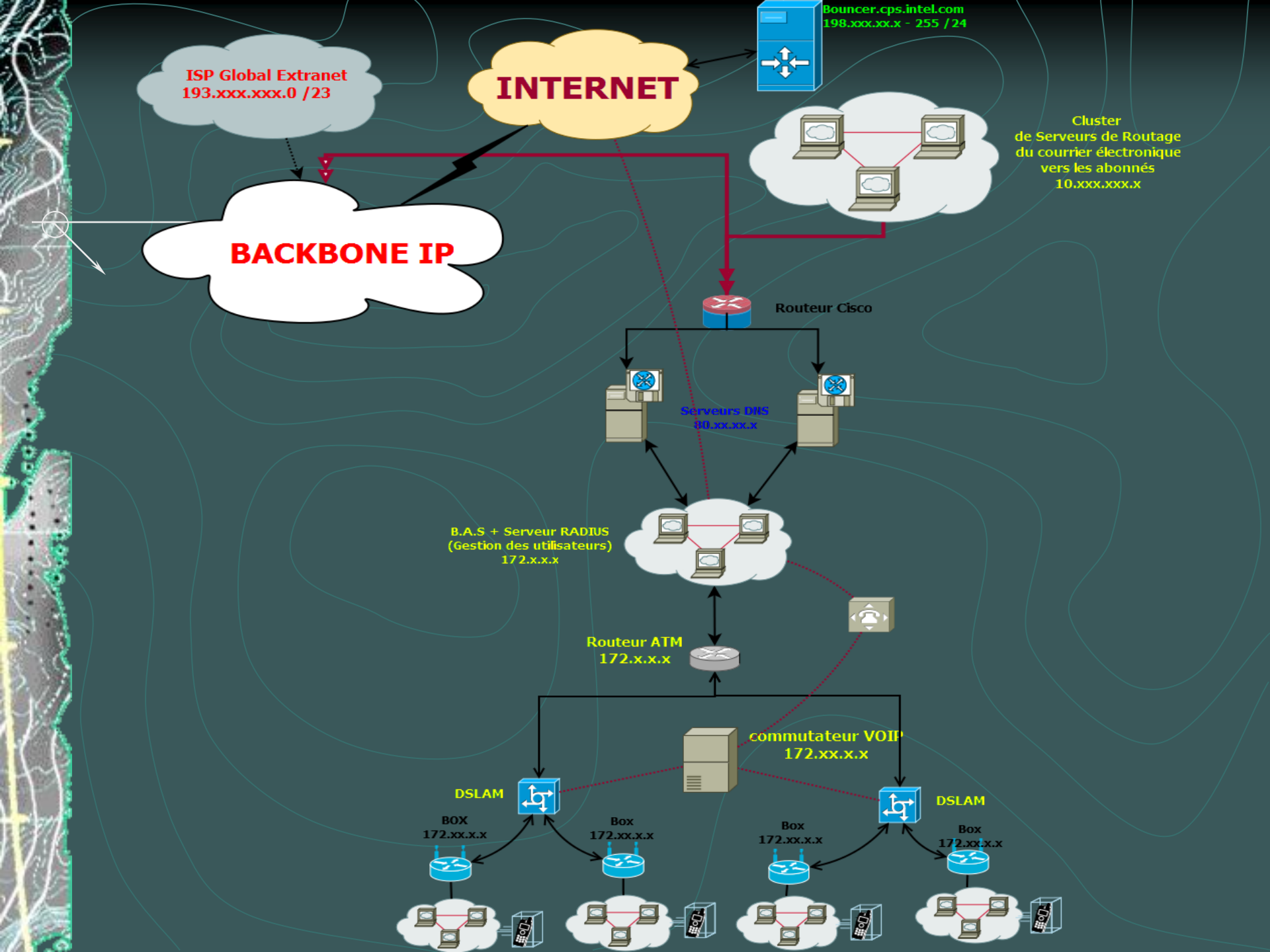
Network mapping

Fourth surprise (Mail servers) :

```
Host 10.xxx.xxx.193 appears to be up.
Host 10.xxx.xxx.194 appears to be up.
Host 10.xxx.xxx.195 appears to be up.
Host 10.xxx.xxx.196 appears to be up.
Host 10.xxx.xxx.198 appears to be up.
Host 10.xxx.xxx.209 appears to be up.
Host 10.xxx.xxx.210 appears to be up.
Host 10.xxx.xxx.211 appears to be up.
Host 10.xxx.xxx.212 appears to be up.
Host 10.xxx.xxx.213 appears to be up.
Host 10.xxx.xxx.214 appears to be up.
Host 10.xxx.xxx.215 appears to be up.
Host 10.xxx.xxx.216 appears to be up.
Host 10.xxx.xxx.217 appears to be up.
Host 10.xxx.xxx.218 appears to be up.
Host 10.xxx.xxx.219 appears to be up.
Host 10.xxx.xxx.220 appears to be up.

OS guesses: Mirapoint Messaging Operating System 3.6.5 (96%)
```

and so much more ...


Bouncer.cps.intel.com
198.xxx.xx.x - 255 /24
ISP Global Extranet
193.xxx.xxx.0 /23
INTERNET
Cluster
de Serveurs de Routage
du courrier électronique
vers les abonnés
10.xxx.xxx.x
BACKBONE IP
Routeur Cisco
Serveurs DNS
80.xx.xx.x
B.A.S + Serveur RADIUS
(Gestion des utilisateurs)
172.x.x.x
Routeur ATM
172.x.x.x
commutateur VOIP
172.xx.x.x
DSLAM
DSLAM
BOX
172.xx.x.x
Box
172.xx.x.x
Box
172.xx.x.x
Box
172.xx.x.x

Exploitation

- Possible attacks (ISP side) :
  - Man in the Middle
  - DNS Spoofing
  - ID spoofing like :

```
503 5.5.0 polite people say HELO first
HELO
501 HELO requires valid address
HELO postmaster(       fr
250 mwinf5d44 hello [81.      .27], pleased to meet you
```

  - And so much more…..

Aftermatch

- Who are the first victims ?
- What is the impact ?

- What conclusions to draw ?!

Questions ?!?

- Some minutes for questions =)

Thanks

- Mari0 for designing slides
- Phillippe Langlois for advising
- You : If you payes a beer