# tetaneutral.net - Evolution #35

## IPv6

18/07/2011 10:22 - Laurent GUERBY

| | | | |
|---|---|---|---|
| **Statut:** | Fermé | **Début:** | 18/07/2011 |
| **Priorité:** | Normal | **Echéance:** | |
| **Assigné à:** | | **% réalisé:** | 0% |
| **Catégorie:** | | **Temps estimé:** | 0.00 heure |
| **Version cible:** | | | |

**Description**

- activation a Myrys via CISCO => fait par Marc 20110716
- faire un backup du CISCO sur une VM
- Filtrage RA et DHCPv6 en iptables, stagiaire potentiel en aout 2011

### Historique

#### #1 - 22/07/2011 14:49 - Laurent GUERBY

En pratique il s'agirait d'etudier les RFC sur le sujet
et d'en traduire une partie en regles ip6tables / ebtables
pour une mise en production sur nos serveurs.

http://tools.ietf.org/html/rfc4890
Recommendations for Filtering ICMPv6 Messages in Firewalls

http://tools.ietf.org/html/rfc6092
Recommended Simple Security Capabilities in Customer Premises Equipment
for Providing Residential IPv6 Internet Service

Il faudrait aussi tester le fonctionnement des clients "classiques"
Microsoft Windows, MacOS, Linux & autres dans un environnement ou l'IPv6
est activé, et mettre en place des outils de surveillance et d'alerte
liés a l'IPv6 en plus des regles de securisation.

#### #2 - 24/07/2011 17:27 - Laurent GUERBY

http://lists.tetaneutral.net/listinfo/ipv6
http://lists.tetaneutral.net/pipermail/ipv6/

#### #3 - 06/08/2011 13:27 - Laurent GUERBY

From: clément Game <clement@digi-nation.com>
<<
Je me permet de forwarder un lien qui est apparu hier soir sur la ML bugtraq, et qui pourrait intéresser nombre d'entre vous. il s'agit d'un document de 160 slides traitant de la sécurité du protocol IPv6, issu d'une conference donnée a HIP 2011..pour tout vous dire je n'ai pas fini de le lire, mais de ce que j'ai parcouru c'est très instructif

le lien: http://www.hackingipv6networks.com/past-trainings

From: Stephane Bortzmeyer <bortzmeyer@nic.fr>
<<
Déjà donné à LACNOG l'année dernière
<http://www.gont.com.ar/talks/lacnog2010/fgont-lacnog2010-ipv6-security.pdf>.
On trouve d'ailleurs quelques hispanismes dans les transparents
(optional écrit opcional).

Du point de vue pratique, c'est un bon document (l'auteur connait son
sujet, et, au fait, il s'est aussi attaqué à IPv4, cf. RFC 6274). Mais
attention à ne PAS s'en servir pour une ÉVALUATION d'IPv6, car il
mélange des problèmes fondamentaux d'IPv6 (SLAAC), d'autres qui ne
sont que conjoncturels (manque de maturité de certaines
implémentations) et d'autres qui sont communs à v4 et v6 (GTSM, mais
aussi le fait que ND est exactement aussi sûr - ou, plus justement,
aussi peu sûr - qu'ARP).

La phrase sur le DNS en bas du transparent 129 est du pur FUD. On voit

qu'il ne connait pas ce sujet (qui n'est pas développé) et qu'il n'a même pas fait d'arithmétique élémentaire.

Il a l'approche de pas mal de spécialistes en sécurité, qui est de considérer la sécurité comme un but en soi. C'est bien résumé dans sa phrase (transparent 165) « The security implications of IPv6 should be considered before it is deployed (not after!). ». Si on avait suivi un tel conseil pour IPv4, on n'aurait pas d'Internet...

---
Liste de diffusion du FRnOG
http://www.frnog.org/

#### #4 - 13/11/2011 12:23 - Laurent GUERBY

http://www.ietf.org/rfc/rfc4890.txt

#### #5 - 13/11/2011 16:35 - Laurent GUERBY

http://madduck.net/docs/ipv6/

#### #6 - 13/11/2011 16:37 - Laurent GUERBY

http://marc.info/?l=linux-kernel&m=123617372002934&w=2

I took another look at
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=blob;f=include/linu \
x/inetdevice.h;hb=HEAD#l102

```
102 #define IN_DEV_RX_REDIRECTS(in_dev) \
103         ((IN_DEV_FORWARD(in_dev) && \
104           IN_DEV_ANDCONF((in_dev), ACCEPT_REDIRECTS)) \
105          || (!IN_DEV_FORWARD(in_dev) && \
106           IN_DEV_ORCONF((in_dev), ACCEPT_REDIRECTS)))
```

"accept_redirect" depends on "forwarding": If forwarding is enabled, it's ANDed, if it's disabled, it's ORed.

#### #7 - 13/11/2011 16:38 - Laurent GUERBY

http://tldp.org/HOWTO/Linux+IPv6-HOWTO/proc-sys-net-ipv6..html

#### #8 - 13/11/2011 16:43 - Laurent GUERBY

http://www.mjmwired.net/kernel/Documentation/networking/ip-sysctl.txt

#### #9 - 13/11/2011 16:49 - Laurent GUERBY

http://ndpmon.sourceforge.net/docs/html/index.html

Pour corriger un RA incorrect : Sent prefix zero lifetime advertisement for wrong prefix.

#### #10 - 13/11/2011 17:18 - Laurent GUERBY

http://getipv6.info/index.php/Customer_problems_that_could_occur

#### #11 - 13/11/2011 17:43 - Laurent GUERBY

http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/

scapy RA generation

http://www.packetlevel.ch/html/scapy/scapyipv6.html

https://github.com/strattg/rafixd

scapy rogue RA killer

```
#!/usr/bin/env python
from scapy.all import *
def ra_monitor_callback(pkt):
```

```
 if ICMPv6ND_RA in pkt and pkt[ICMPv6ND_RA].routerlifetime > 9000:
 send(IPv6(src=pkt[IPv6].src)/ICMPv6ND_RA(routerlifetime=0) )
 u = pkt.sprintf("rogue %Ether.src% %IPv6.src% > %IPv6.dst% %ICMPv6ND_RA.routerlifetime%")
 s = time.asctime()
 t = "\t"
 return s + t + u

sniff(prn=ra_monitor_callback, filter="dst host ff02::1", store=0, iface="wlan0")
```

#### #12 - 10/08/2018 09:08 - Matthieu Herrb

*- Statut changé de Nouveau à Fermé*

fermeture de tous les vieux tickets non suivis depuis plusieurs années