Attaque de type Man-In-The-Middle sur réseau «dual-stack»

Global Security Days – 24 mars 2015

SUDKI Karim

Introduction | Agenda

Introduction

Rappel IPv6

Théorie de l'attaque

pyMITM6

Conclusion

Q&A

Introduction | Whoami

[SUDKI Karim]

Ingénieur sécurité @SCRT (2013)

[SCRT]

Organisateur d' Insomni'Hack
19-20 mars, Genève

Partenaire de la St'Hack
27 mars, Bordeaux

STHACK
Ethical Hacking | CTF & Conférences

Introduction | Subject

[Actualité]
2011 PoC SLAAC Attack
2013 **DEFCON 21**
“MITM all the ipv6 things”
“ Fear the Evil FOCA: IPv6 attacks in Internet Connections ”

[Domaines d’application]
Audits de sécurité
Internet des objets (IoT)

[Intérêt]
Méthode alternative à “ARP Spoofing”

IPv6 | History

[Historique]

90’s – Prédiction épuisement IPv4

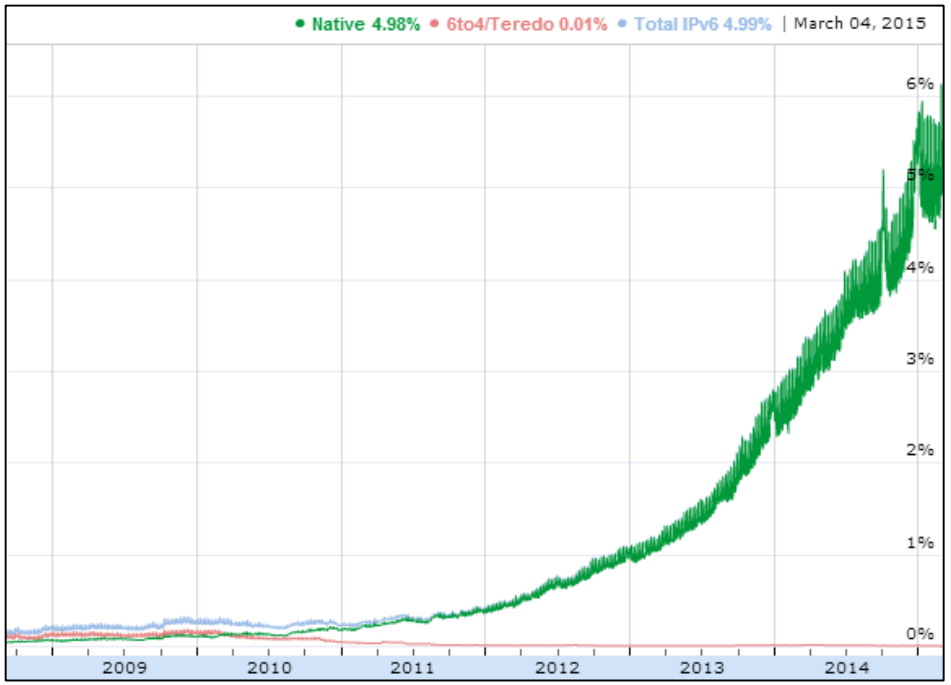
2011 – IPv6 Test Day

2012 – World IPv6 Launch

[Constat]

Maigre utilisation sur Internet

Et dans les réseaux d’entreprise ?

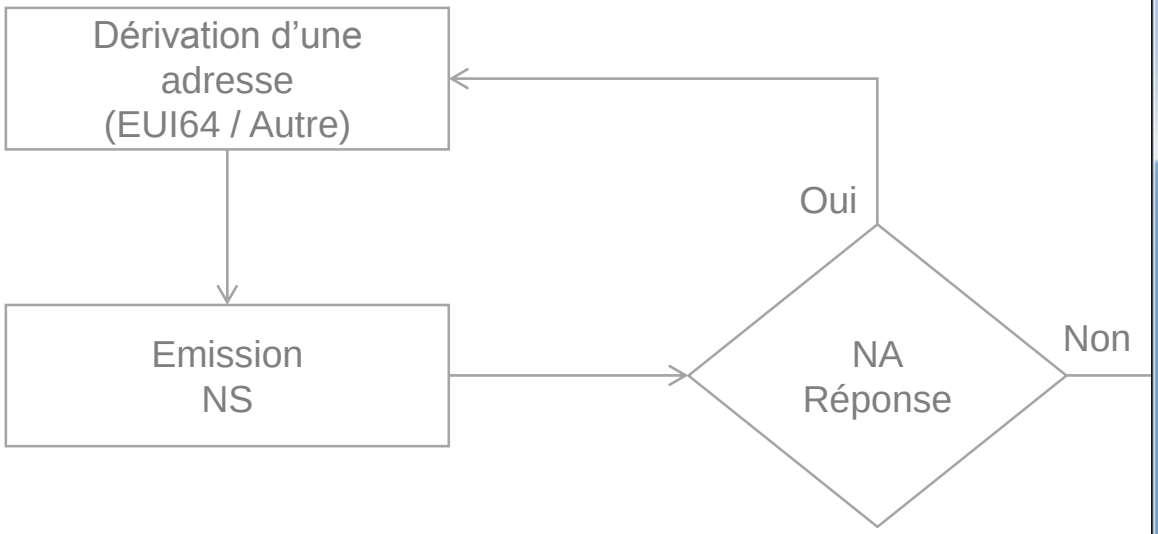


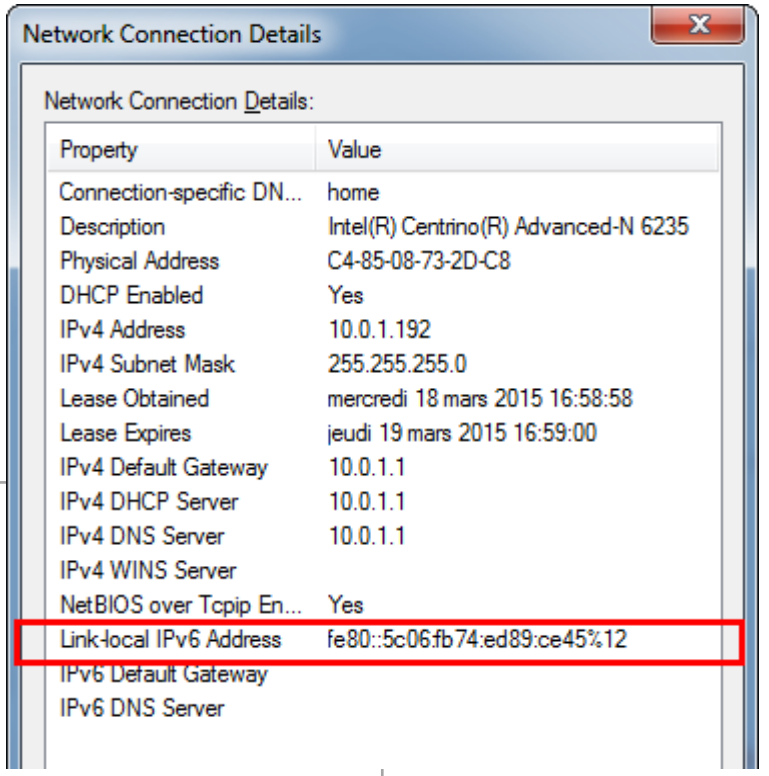
Source: http://www.google.fr/ipv6/statistics.html

IPv6 | Overview

	IPv4	**IPv6**
Adressage	32bits	128 bits
Notations	A.B.C.D	AAAA:BBBB::CCCC:DDDD
Exemples	10.1.0.100	2001::db8:0:1 fe80::0202:b3ff:fe1e:8329
Auto Configuration	DHCP (stateful)	DHCPv6 (stateful) SLAAC (stateless)
Protocole de voisins	ARP	NDP (basé sur ICMPv6) - Router Advertisement (ff02::1) - Router Solicitation (ff02::2) - Neighbour Advertisement (ff02::1) - Neighbour Solicitation (ff02::1:ff00:0)

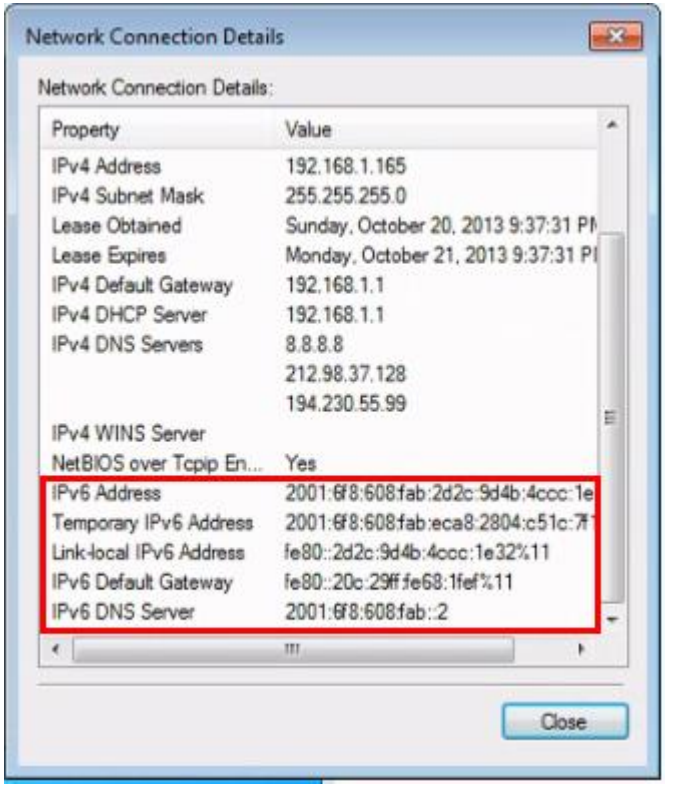
IPv6 | Basic Configuration





Auto configuration

IPv6 | Autoconfiguration



IPv6 | Transition Mecanisms

[Dual Stack]
Communication en IPv4 et/ou IPv6

[Translation d'adresses]
Communication entre noeuds exclusivement IPv4 et IPv6

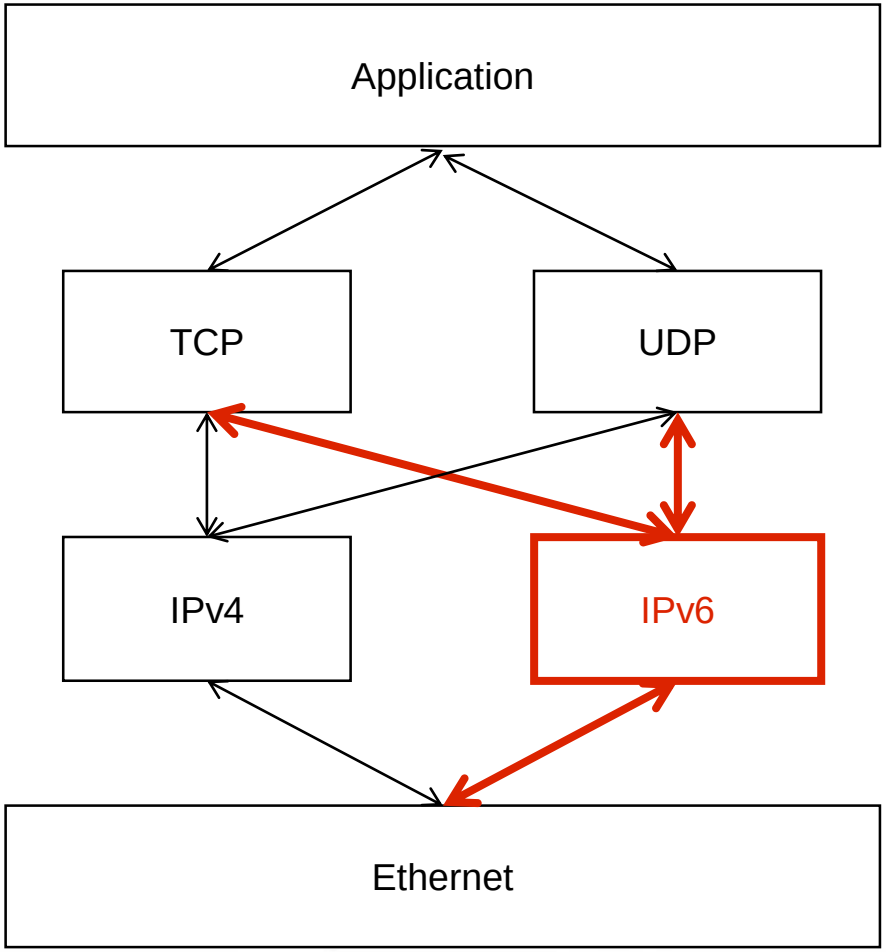
[Tunnels]
Encapsulation de paquets IPv6 pour transport sur réseau IPv4

IPv6 | Transition Mecanisms

[Dual Stack]
Active par défaut (Win, Mac)

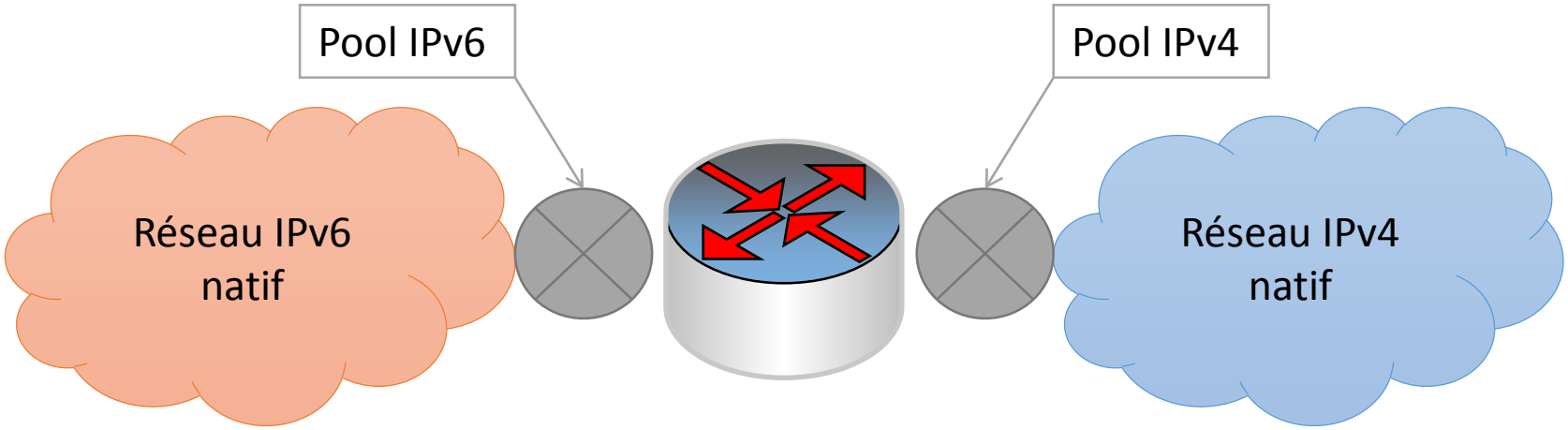
IPv6 préféré automatiquement

Piles indépendantes



IPv6 | Transition Mecanisms

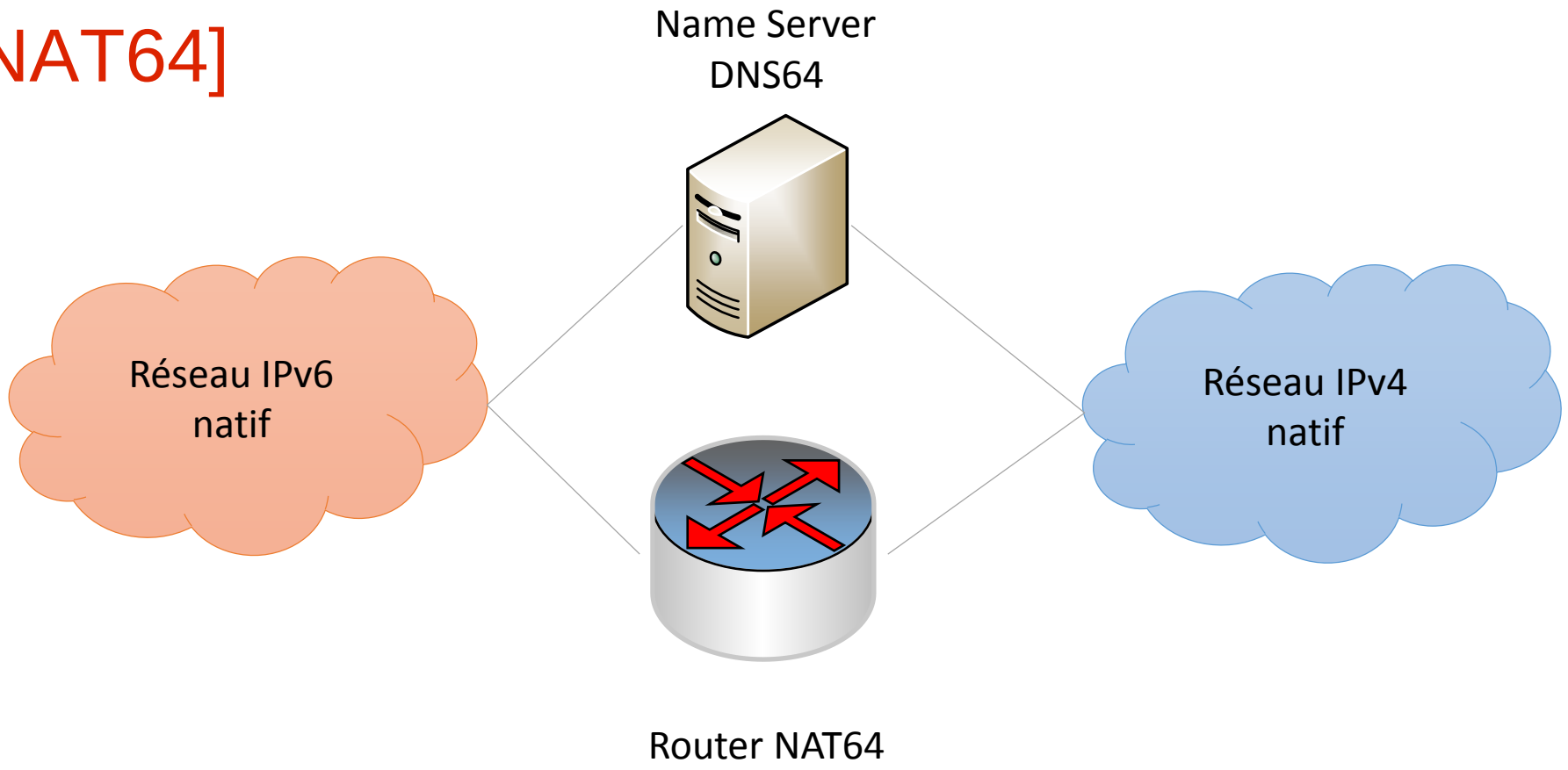
[NAT-PT]



Router NAT-PT
DNS (ALG)

IPv6 | Transition Mecanisms

[NAT64]



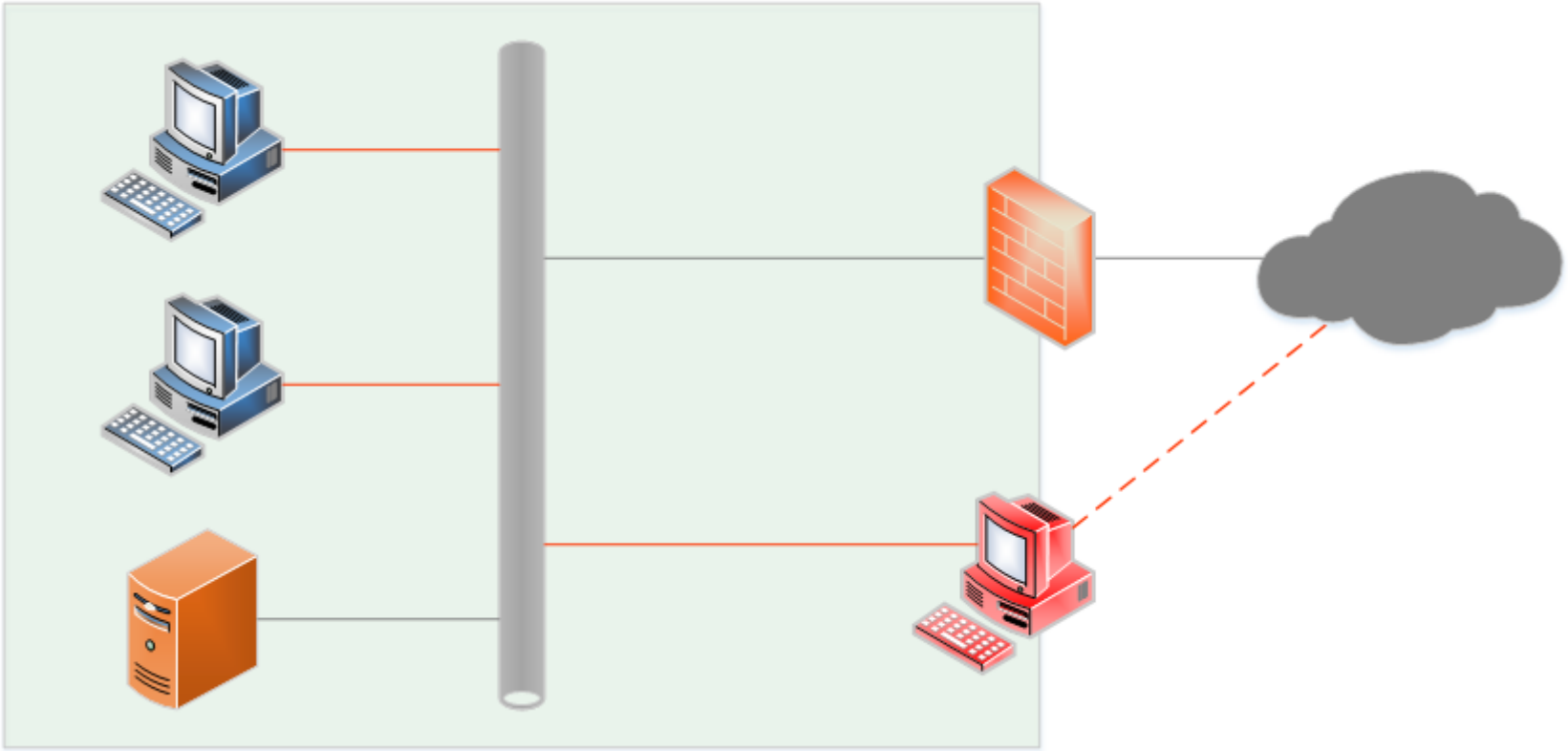
IPv6 | Attacks

Neighbour **A**dvertisement (**NA**) Spoofing

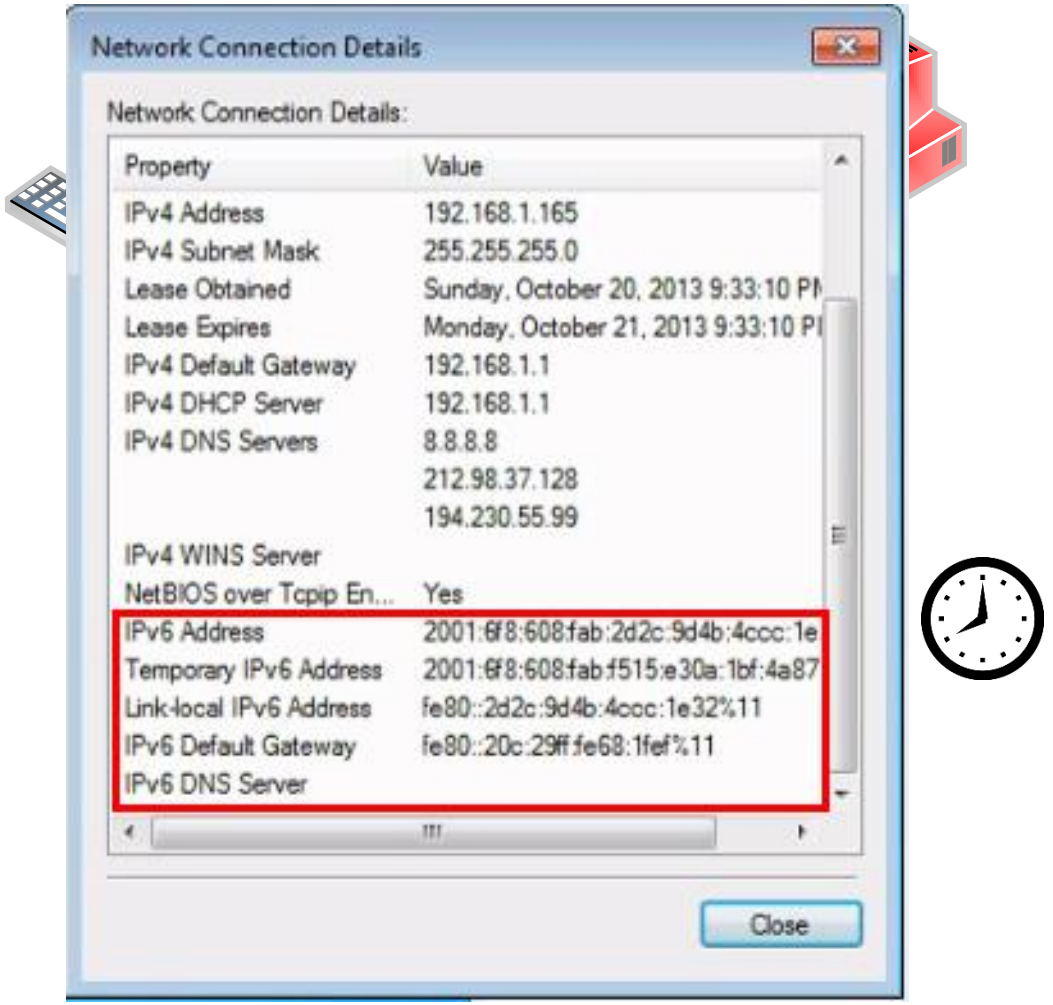
State**L**ess **A**ddress **A**uto **C**onfiguration (**SLAAC**)

Web **P**roxy **A**utodiscovery **P**rotocol (**WPAD**) (idem IPv4)

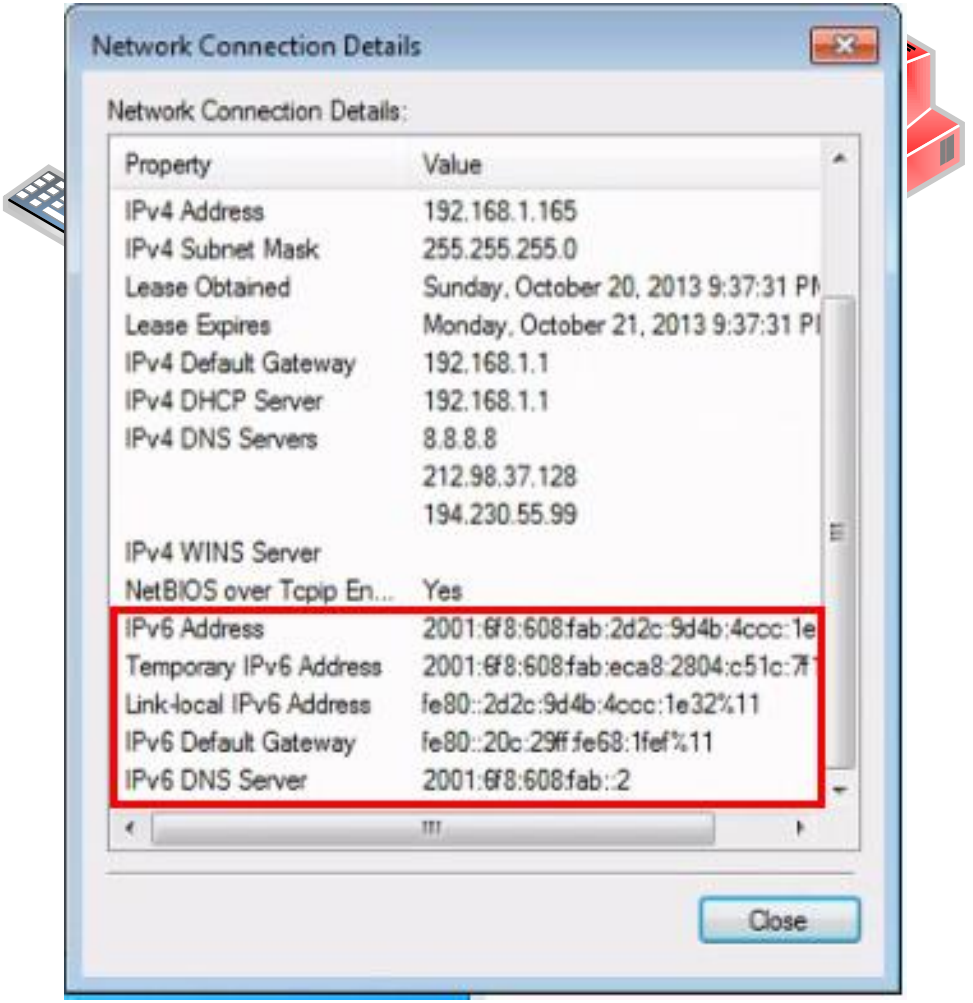
SLAAC Attack | Concept



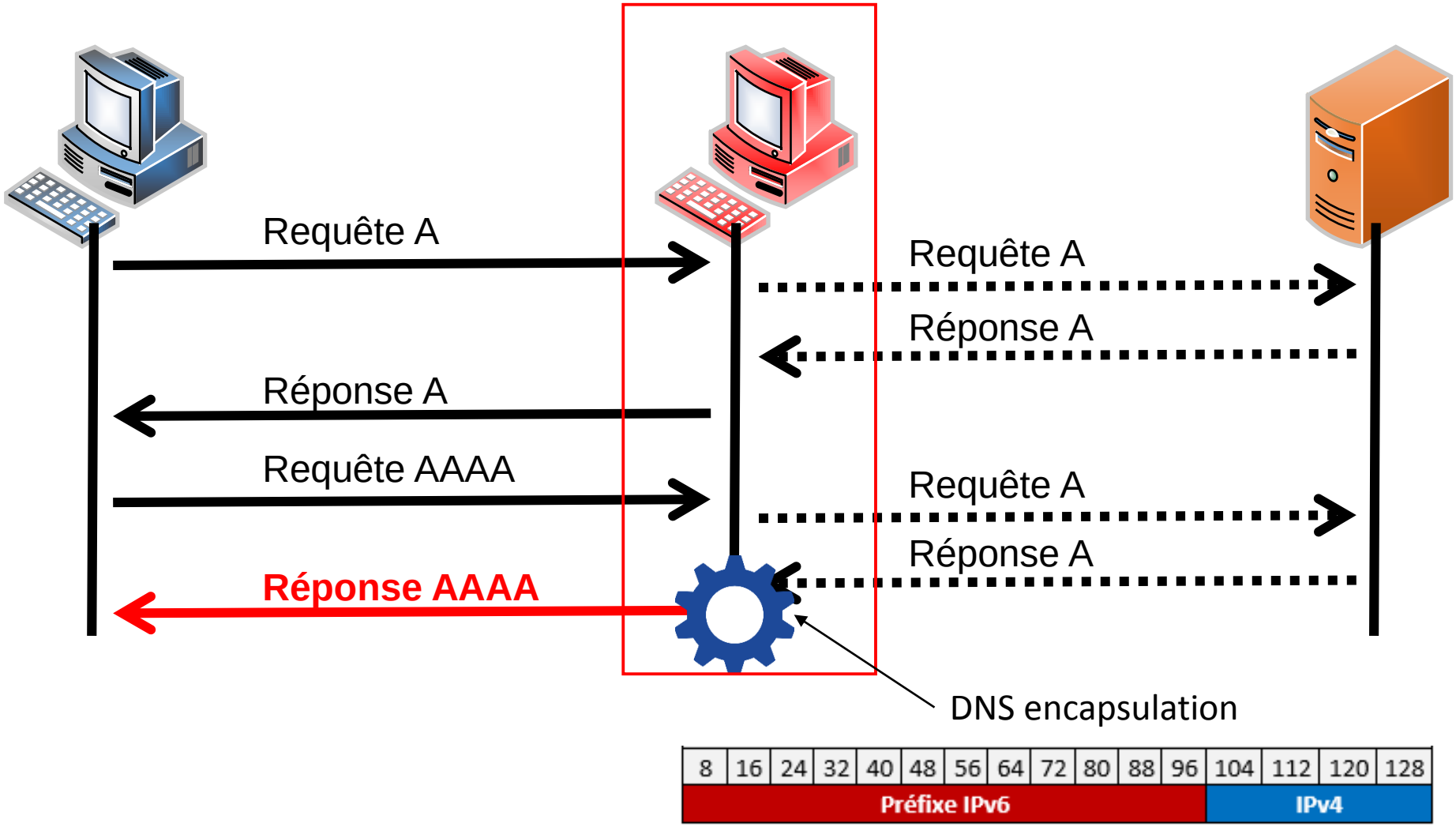
SLAAC Attack | Configuration



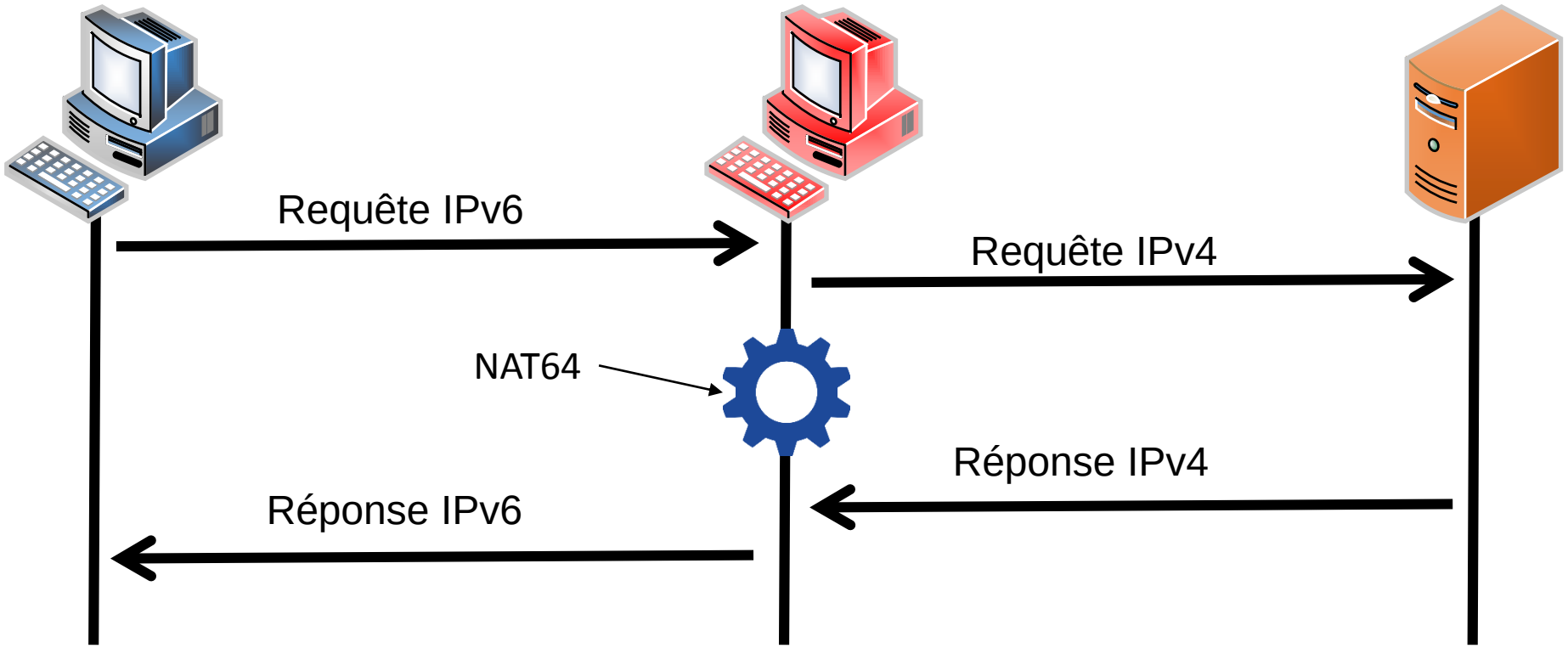
SLAAC Attack | Configuration



SLAAC Attack | Name resolution



SLAAC Attack | Network flow



SLAAC Attack | State of the art

[Suddensix]
Bash script pour automatisation installation + configuration
Utilisation de paquets + protocle NAT-PT obsolètes

[Evil FOCA]
Outil complet (multiples attaques IPv4 & IPv6)
Windows

SLAAC Attack | Wrap-up

[Avantages]
Peu de paquets nécessaires au maintien de l'attaque

Contrôle du flux et du DNS

Sélection des victimes

Moins de protection IPv6 sur réseau IPv4

[Inconvénient]
Mise en œuvre de l'attaque fastidieuse

=> Création d'un outil pyMITM6 <=

pyMITM6 | Introduction

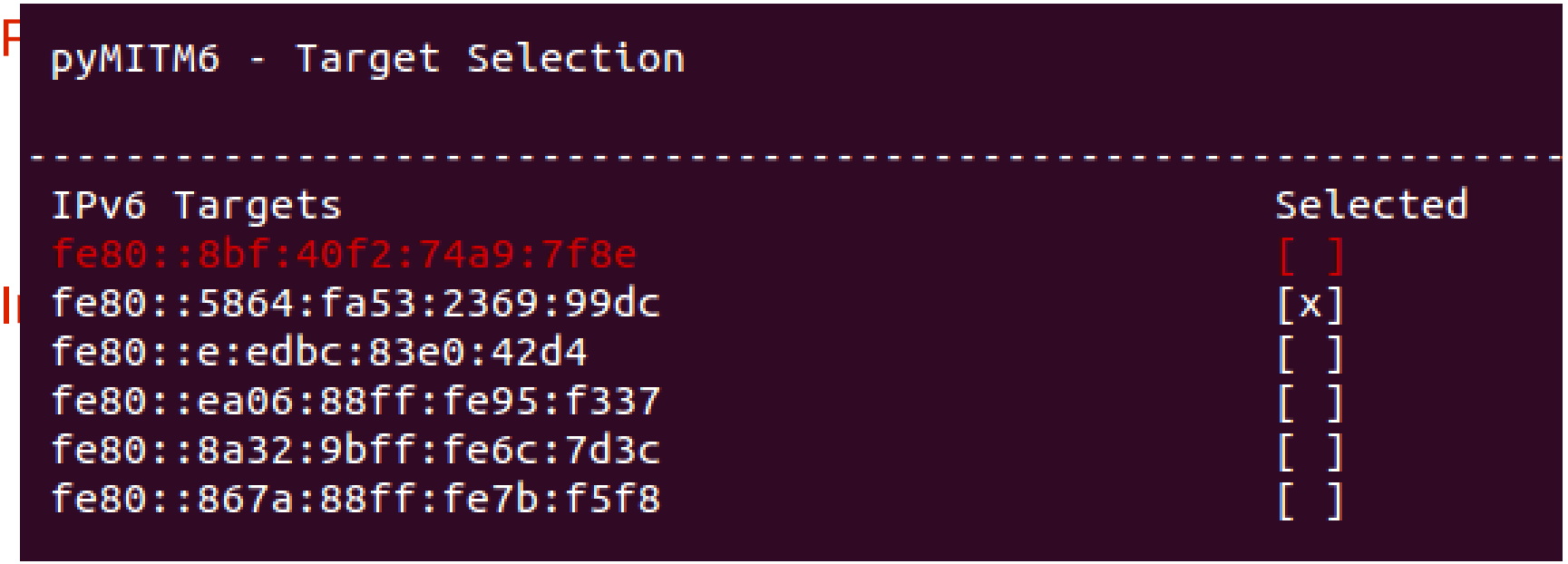
[Développement]

- Python 2.x
- Licence GPLv2
- Utilisation des librairies standards => pas de dépendances

[Modules]

- Interface
- Configuration
- Résolution de noms
- Traduction d’adresses

pyMITM6 | Interface



pyMITM6 | Configuration

[Fonctionnalités]

- Configuration IPv6 de la victime
  - Emission de RA périodiquement
  - Emission de RA en réponse au RS
- Configuration du serveur DNS via DHCPv6 (Info requ.)

[Implémentation]

- Sockets IPv6/raw

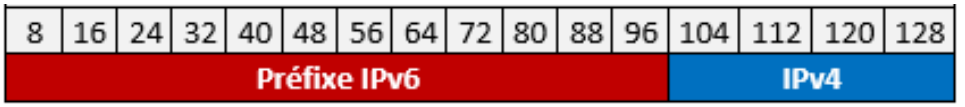
[Prérequis]

- Préfixe IPv6 (config)
- Adresse IPv6 du Serveur DNS

pyMITM6 | Name resolution

[Fonctionnalités]

- Interception requêtes A et AAAA
- Interrogation serveur réel IPv4 ou du cache (requête A)
- Modification pour les réponses AAAA



[Implémentation]

- Librairie python dnslib
- Socket IPv6/udp

[Prérequis]

- Préfixe IPv6 (différent de celui de Configuration)

pyMITM6 | Network Adress Translation

[Fonctionnalités]

- Traduction des adresses IPv6 en IPv4 (vice-versa)

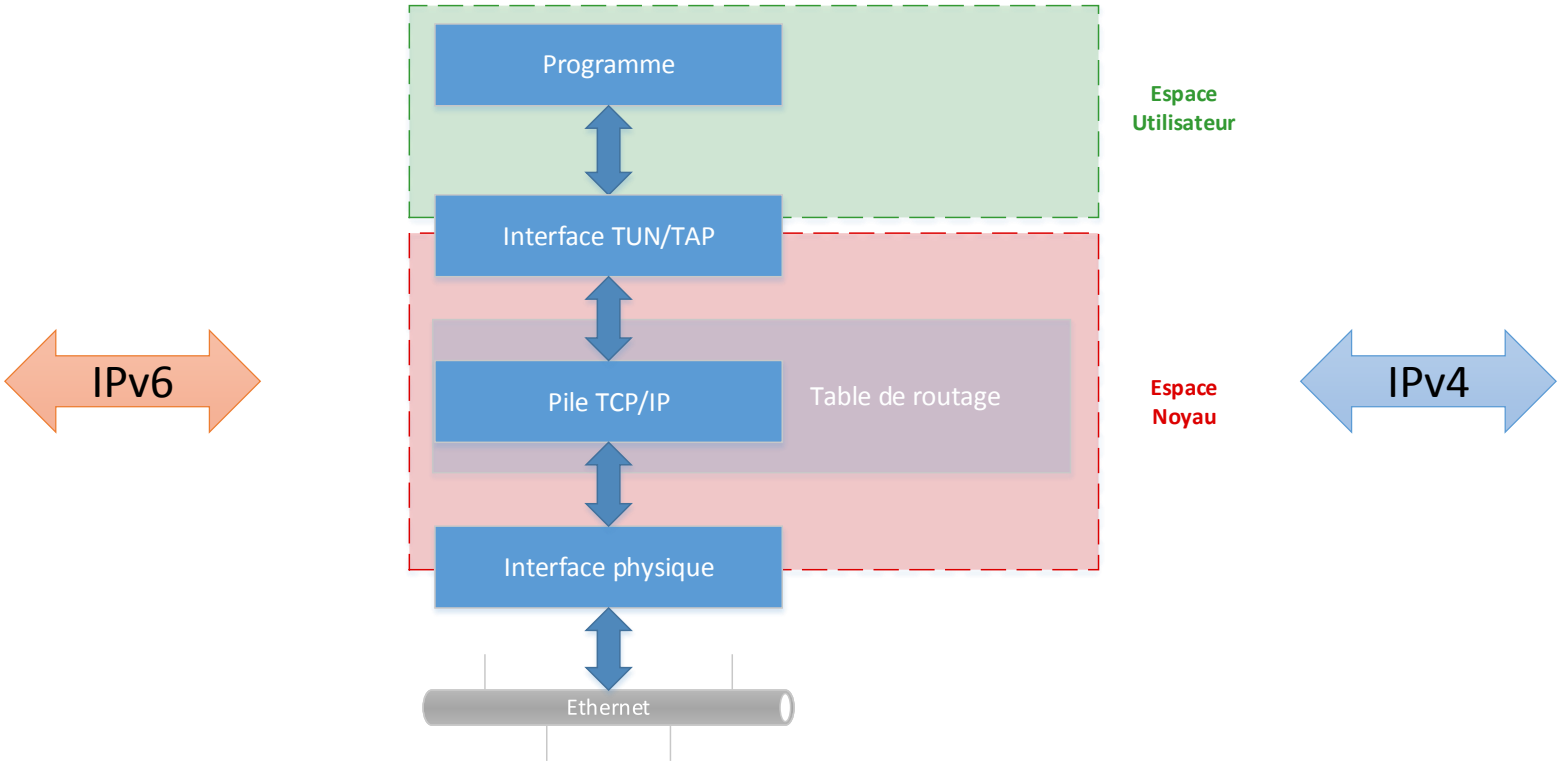
[Implémentation]

- Algorithme SIIT [RFC 2765] (NAT64)
- Routage (linux)
- Interface TUN
- Source NAT (iptables)

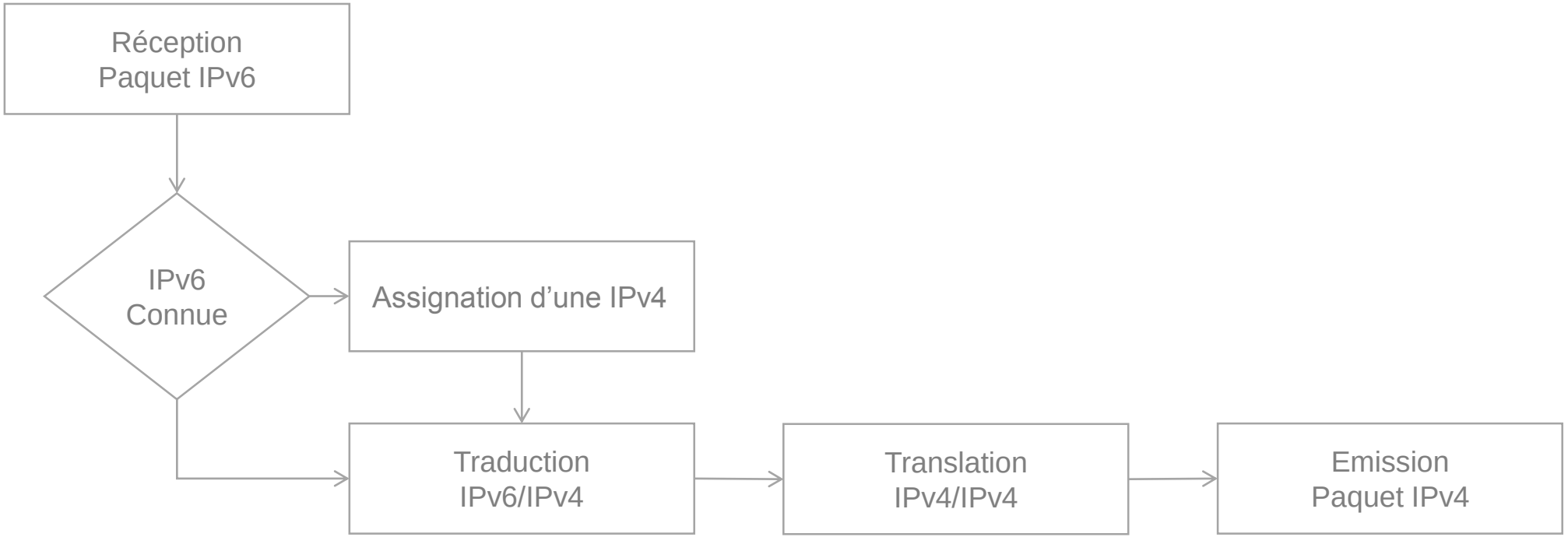
[Prérequis]

- Plage d’adresses IPv4 (fonctionnement interne)

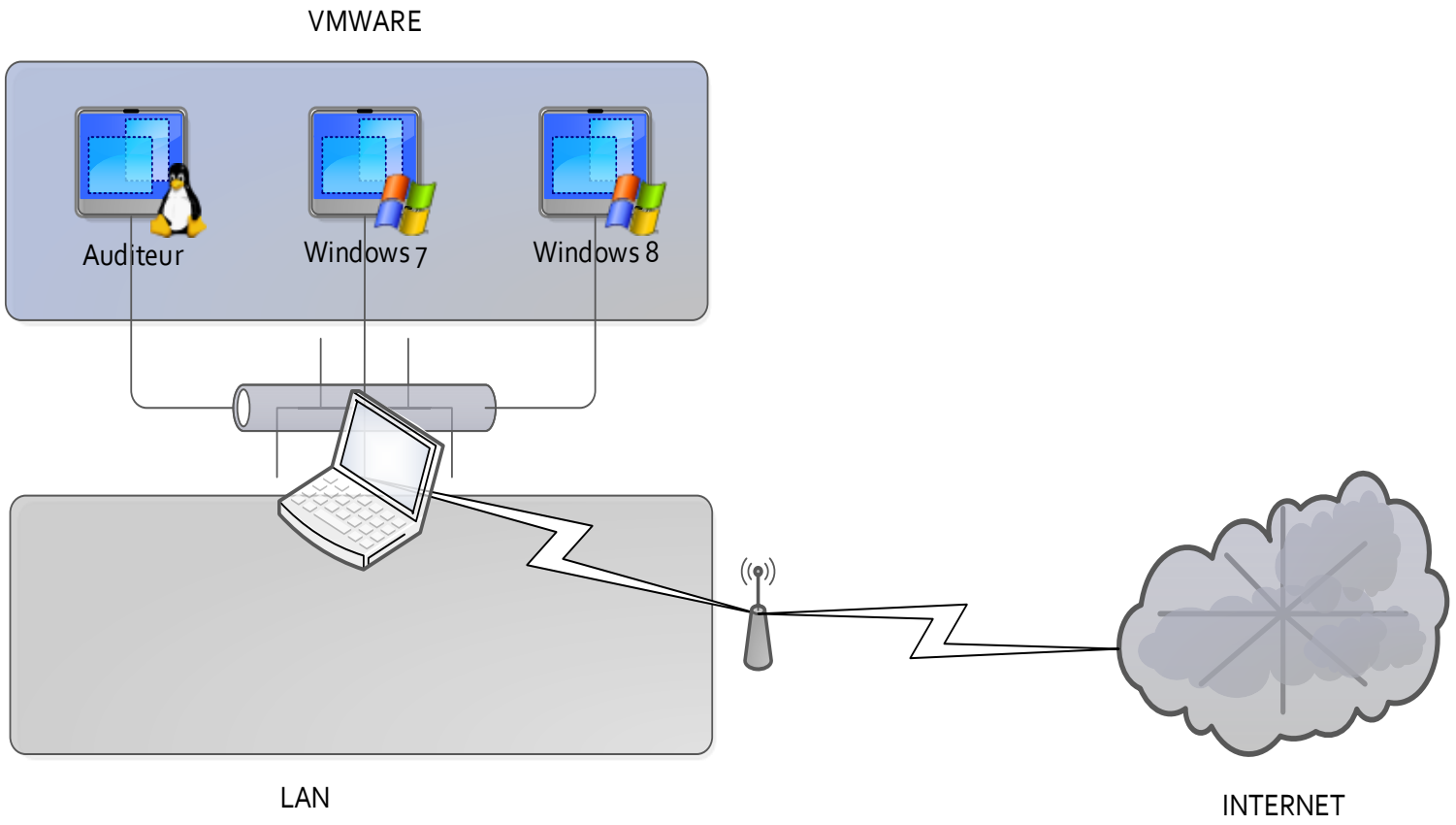
pyMITM6 | Traduction d'adresses



pyMITM6 | Traduction d'adresses



pyMITM6 | Demo



pyMITM6 | Limitations

Contournement des protections (RA Guard)

Améliorer l'implémentation DHCPv6 (Windows Server 2k12)

Interface graphique

WPAD (proxy)

Protections

Désactivation de la pile IPv6

IPv6 Router Advertisement Guard [RFC 6105]

Monitoring NDP (NDPMon)

Conclusion

Attaque alternative à ARP Spoofing

Contrôle du flux réseau

Contrôle de la résolution de noms

Fallback en IPv4 automatique

Protection peu/pas implémentée

Merci

[em@il] karim@scrt.ch
[twitter] @8008135_