

SECURINETS



**CLUB DE LA SECURITE INFORMATIQUE
INSAT**

SECURILIGHT 2011

Ipv6 et sécurité

Chef Atelier : Ibtissem Omar (RT3)

Hajer Meherzi (RT3)

Rania Fliss (RT3)

Hajer Makina(RT3)

Roua Touihri (RT3)

30/11/2011

1) Introduction :

Présentation des notions de base du protocole IP dans sa 6ième version et ses protocoles. une communication de deux réseaux ipv6 ainsi qu'une simulation d'une attaque ipv6.

I. Partie théorique :

Pourquoi l'IPv6 ?

- * Résoudre le problème de pénurie d'adresses d'IPv4.
- * Résoudre les problèmes de dimensionnement des tables de routage .
- * Inclure de nouvelles fonctionnalités
 - nouvelles fonctionnalités
 - le multipoint, la sécurité, la mobilité.
 - La configuration automatique des stations.
 - La qualité de service, etc...

2) Les attaques Ipv6 :

I. Exemple : L'attaque Smurf :

- L'attaquant envoie une trame IP du type ICMP à tous les nœuds du lien du réseau cible .
- Lorsque la trame arrive sur le réseau cible, tous les périphériques la réceptionnent et la considèrent. Ils l'interprètent tous individuellement comme si elle leur était directement adressée
- Les périphériques du réseau cible vont répondre à l'IP source de la trame reçue correspondant à la cible visée. La réponse sera bien sûr envoyée n fois correspondant au nombre d'hôte sur le LAN répondant au broadcast

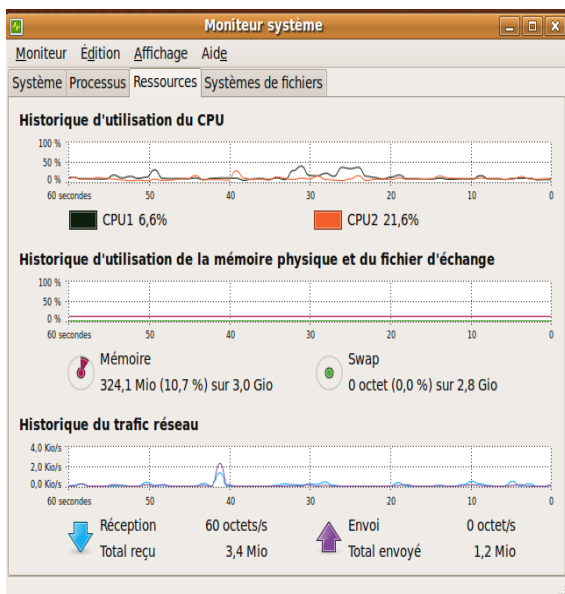
II. Partie pratique :

- pour lancer cette attaque, on fait :

smurf6 interface-attaquant adresse_victime

- on a visualisé l'utilisation de la mémoire avant et après le lancement de l'attaque smurf.

Avant l'exécution de SMURF6



Après l'exécution de SMURF6

