NTP

AFRICA
INTERNET
SUMMIT'18
DAKAR SENEGAL
29 APRIL - 11 MAY 2018

NTP

AFRICA INTERNET SUMMIT'18

DAKAR SENEGAL

29 APRIL - 11 MAY 2018

Bonjour.. Qui suis-je ?

- Nitin J Mutkawoa (Nitin)
- Membre du groupe hackers.mu (#3)
- Cloud Solutions Engineer @ Orange Cloud for Business – Orange Business Services
- Champion à IETF 101 (TLS 1.3)

- Je vis à Tunnelix.com
- Twitter: @TheTunnelix
- FB: Facebook.com/TunnelixDOTCom
- E-mail: jmutkawoa@hackers.mu

Contribution OpenSource à ce jour

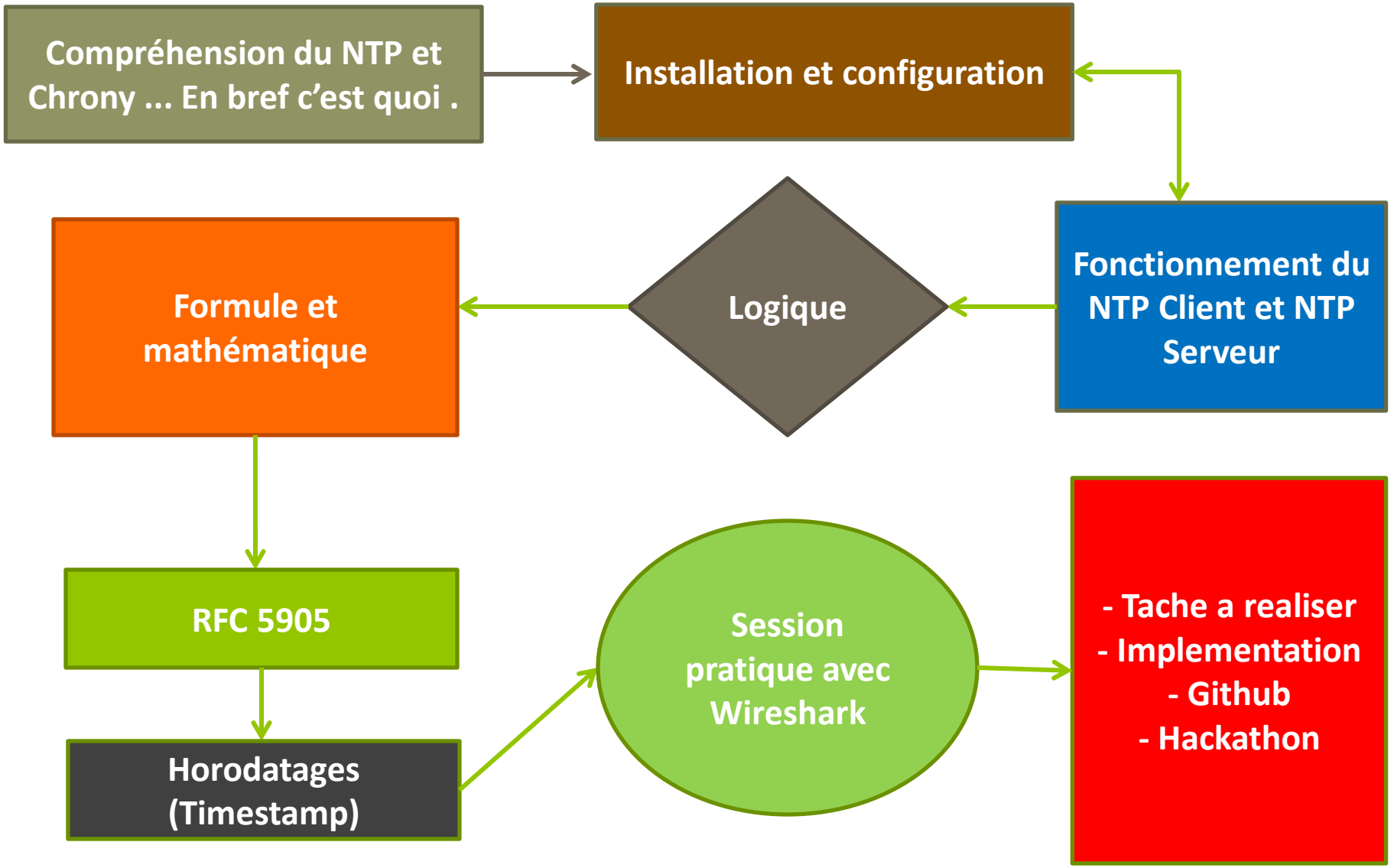
Nagios®

stunnel

Firejail Security Sandbox

Quelques membres du groupe hackers.mu

Plan de Vol


Compréhension du NTP et Chrony ... En bref c'est quoi .
Installation et configuration
Fonctionnement du NTP Client et NTP Serveur
Logique
Formule et mathématique
RFC 5905
Horodatages (Timestamp)
Session pratique avec Wireshark
- Tache a realiser
- Implementation
- Github
- Hackathon

Installation et configuration

- NTP client sur Ubuntu / CentOS
- NTPD vs Chrony
- Chronyd est une évolution de NTPD, et fonctionne généralement mieux pour la synchro et de haute précision (Drift).
- Installation

Network Time Protocol

La logique du protocole NTP ?

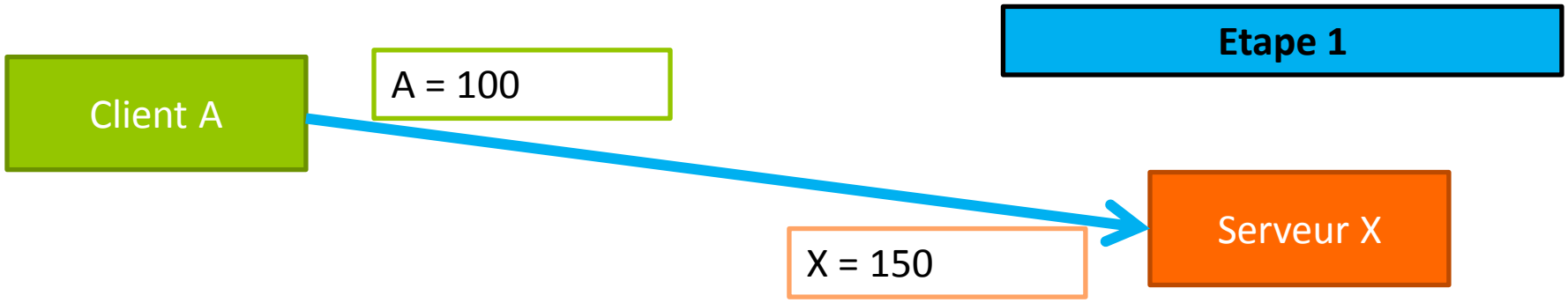
- Le client NTP envoie une requête avec un horodatage.

- Le serveur NTP retourne le paquet avec 3 horodatages.

    1. écho de l'horodatage du client
    2. L'horodatage reçu par le serveur
    3. La réponse d'horodatage envoyée par le serveur.

- Le client va alors estimer le décalage (la différence d'horodatage entre le client et le serveur)

A vos stylos à vos papiers et c'est parti !!!

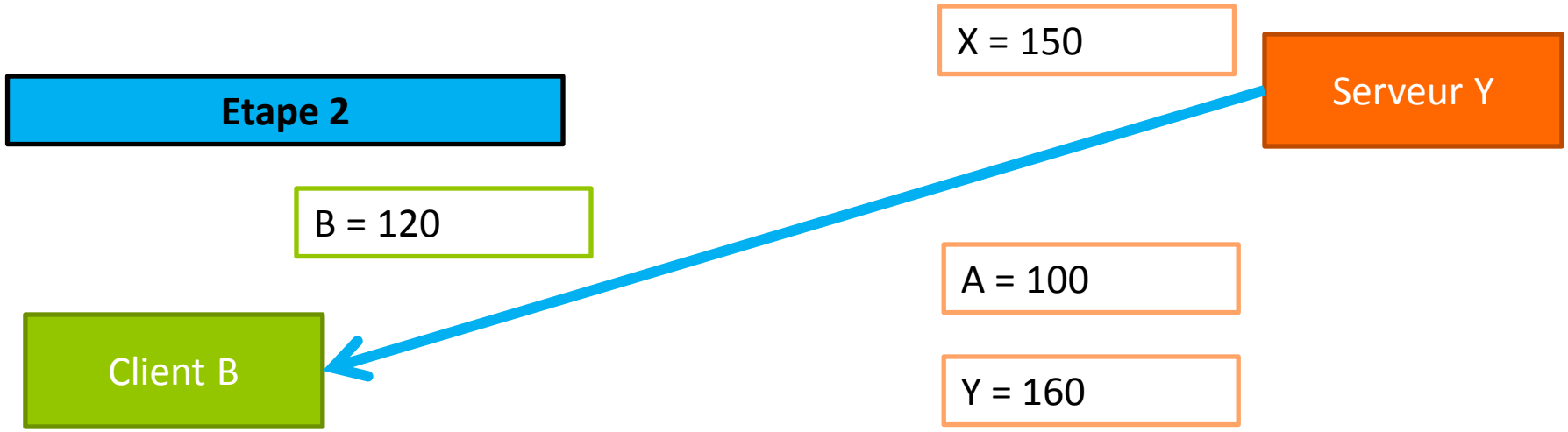


Comprendre en parti ce qui se passe dans l'algorithme

Le Client NTP envoie une demande au serveur X - Supposons A = 100 où 100 est l'heure du client.

Le serveur NTP X a reçu la requête après quelques secondes. - Supposons X = 150 où 150 est l'heure du serveur.

A vos stylos à vos papiers et c’est parti !!!



Étant donné que la demande du client NTP n'est pas nécessairement servit immédiatement, il y a un lapse de temps à ce stade. Supposons que X est maintenant a 160.

Nous avons maintenant 3 valeurs, c'est-à-dire , l'heure à laquelle le client a envoyé la demande, l'heure (en temps réel) à laquelle le serveur a reçu la demande et l'heure à laquelle le serveur veut répondre.

Maintenant, le client NTP récupère la demande à 120. C'est parce que le client NTP a son propre temps.

Comment le client déterminera le temps nécessaire pour obtenir la réponse du serveur?

$$\frac{[(B - A) - (Y - X)]}{2}$$

$$\frac{[(120 - 100) - (160 - 150)]}{2}$$

$$\frac{[20 - 10]}{2}$$

$$= 5$$

Le client ajoute 5 secondes à l'heure du serveur au moment où il reçoit une réponse, ce qui fait 160 +5 = 165 secondes.

Le client sait qu'il doit ajouter 45 secondes à son horloge. Ceci est fait en réduisant de 165 - 120 = 45 secondes. Où 45 secondes est la différence entre le client et l'horloge du serveur auquel le client mettra son horloge en avant de 45 secondes (Drift).

Horodatage et RFC 5905

- Surveillance en masse (Pervasive Monitoring)
- Confidentialité (Privacy)
- Horodatage – Paquet en mode 3
- Notre but aujourd'hui et de sécuriser le client NTP
- Outils – Wireshark

NTP

Network Time Protocol

Merci à tous