NTP

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

NTP

AFRICA INTERNET SUMMIT'18

DAKAR SENEGAL

29 APRIL - 11 MAY 2018

Hello.. Who am I ?

- Nitin J Mutkawoa (Nitin)
- Member of team hackers.mu (#3)
- Cloud Solutions Engineer @ Orange Cloud for Business – Orange Business Services
- Champion at IETF 101 (TLS 1.3)

- I live at Tunnelix.com
- Twitter: @TheTunnelix
- FB: Facebook.com/TunnelixDOTCom
- E-mail: jmutkawoa@hackers.mu

OpenSource contribution since today

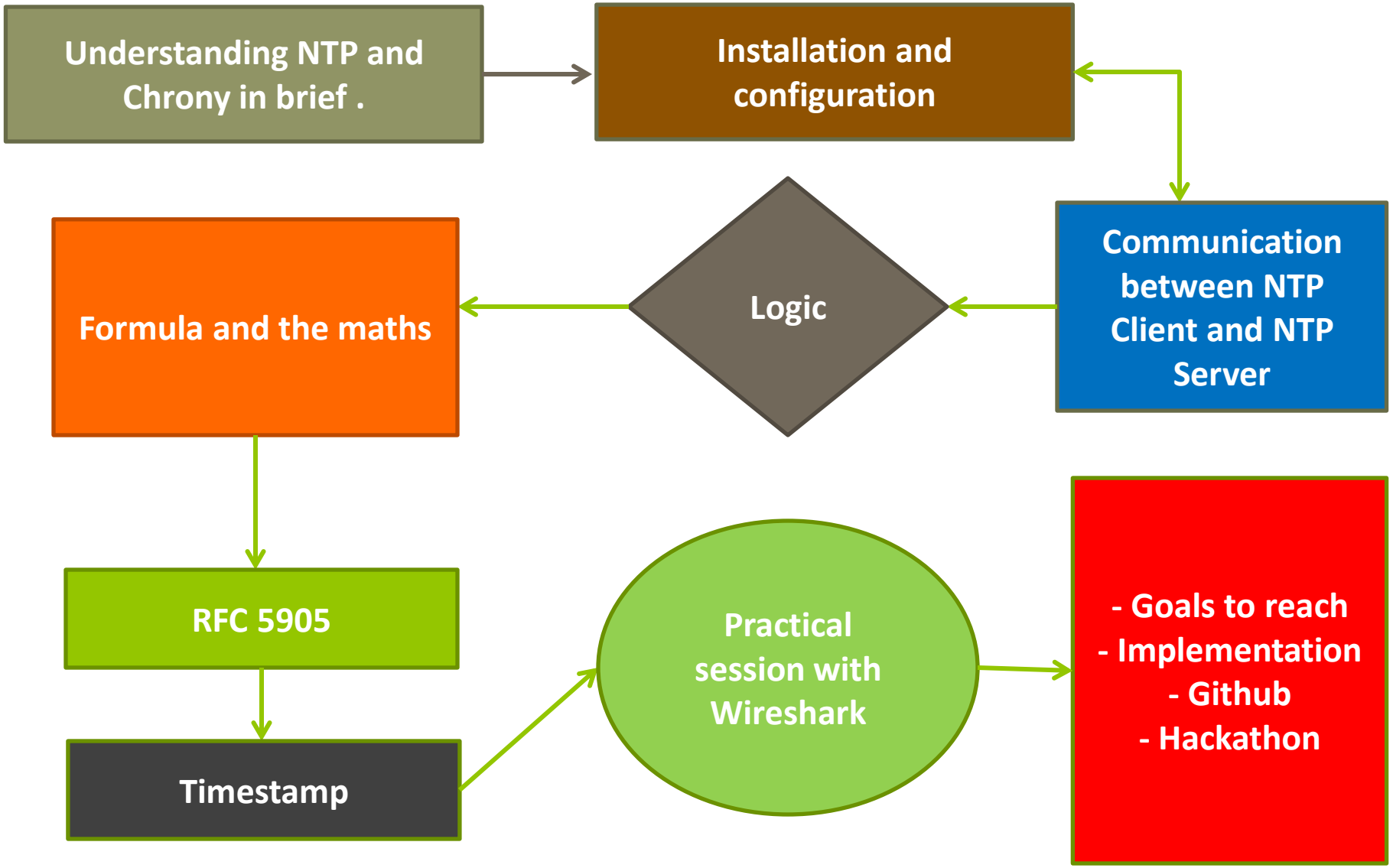
Nagios®

stunnel

Firejail Security Sandbox

Some members from hackers.mu

The plan to success



Installation and configuration

- NTP client on Ubuntu / CentOS
- NTPD vs Chrony
- Chronyd is an evolution of NTPD, and works pretty well in terms of time synchronization and precision (Drift).
- Installation

Network Time Protocol

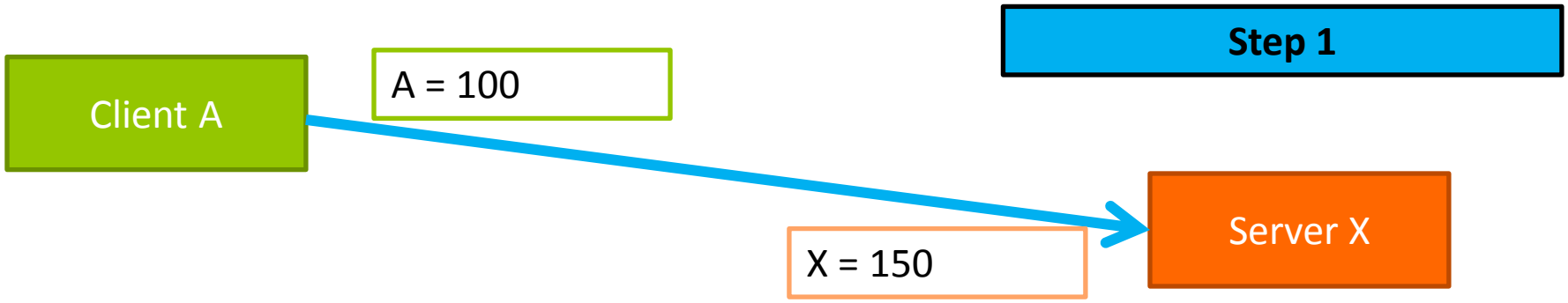
The logic behind NTP ?

- The NTP client send a request with a timestamp.

- The NTP server reply back with 3 timestamps
    1. Echo of timestamp of client
    2. Echo of received timestamps of the server.
    3. Echo of timestamp the server is replying.

- The client will then estimate the difference of time between the server and itself.

Ready – Pen to Paper !!!

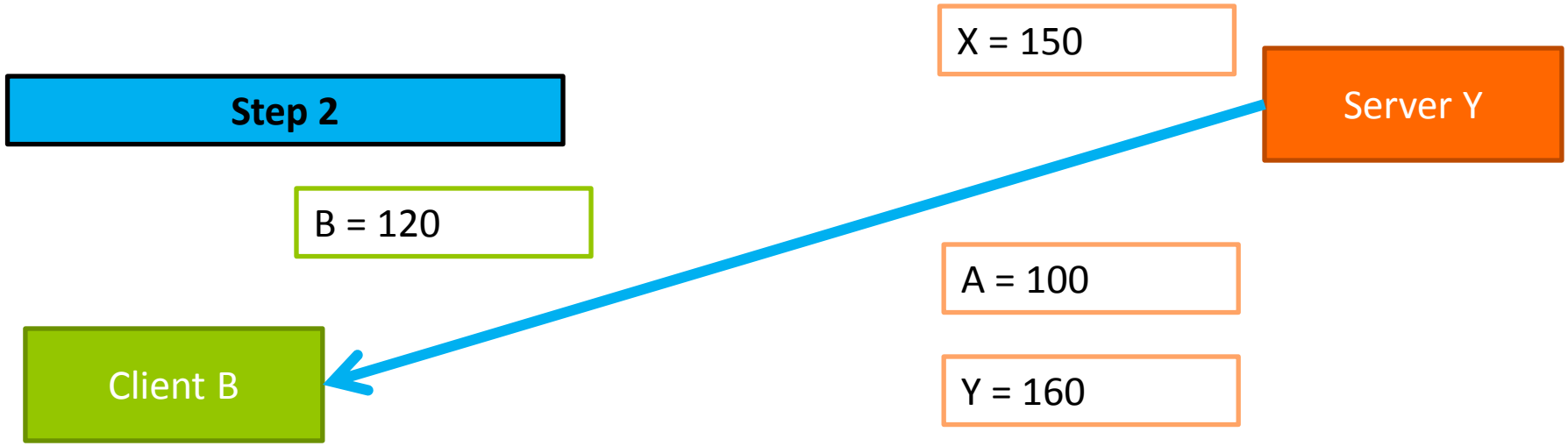


Understanding partly the algorithm behind

NTP Client A send request to server X - Let's assume A=100 where 100 is the time of the client.

NTP Server X received the request after some secs. - Let's assume X= 150 where 150 is the time of the server.

Ready – Pen to Paper !!!



Being given that, the request from NTP client is not necessarily served immediately, there is lapse of time at this point. let's assume that X is now 160.

We now have 3 values i.e; The time the client sent the request, the time (real time) the server received the request and the time the server want to respond back.

Now the NTP client gets the request back at 120. This is because the NTP client has its own time.

How will the client determine the time required to get the server response?

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

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

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

$$= 5$$

Now the client adds 5 seconds to the server time at the time it received the response which makes 160 +5 = 165 seconds.

The client knows it needs to add 45 seconds to its clock. This is done by subtracting 165 - 120 = 45 seconds where 45 seconds is the difference between the client and the server clock to which the client will set forward its clock by 45 seconds (Drift).

Timestamps and RFC 5905

- Pervasive Monitoring
- Privacy
- Timestamps – Packet on mode 3
- Our goal today is to solve the privacy and security issues.
- Tools – Wireshark

NTP

Network Time Protocol

Thank you