

HACKATHON @AIS NTP



— AFRICA —
INTERNET
— SUMMIT'18 —

DAKAR SENEGAL
29 APRIL - 11 MAY 2018

PRESENTATION

SWAM

- Soukeye FAYE
- Wendwosen ABEBE
- Ahmadou SECK
- Mathias HOUNGBO

INTRODUCTION

- Après lecture du **draft-ietf-ntp-data-minimization-00**, deux problèmes ont été identifiés:
 - *Le transmit 'timestamp' permettrait d'identifier un ordinateur dans le réseau*
 - *Le client envoie de nombreuses informations inutiles dans sa requête*

Pour résoudre ces problèmes, des modifications ont été apportées au code source du script <https://github.com/Tipoca/ntplib/>

I. TRANSMIT 'TIMESTAMP'

Code initial

```
347 █
348 def system_to_ntp_time(timestamp):
349     """Convert a system time to a NTP time.
350
351     Parameters:
352     timestamp -- timestamp in system time
353
354     Returns:
355     corresponding NTP time
356     """
357     return timestamp + NTP.NTP_DELTA
358
```

Code modifié

```
354
355 def system_to_ntp_time(timestamp):
356     """Convert a system time to a NTP time.
357
358     Parameters:
359     timestamp -- timestamp in system time
360
361     Returns:
362     corresponding NTP time
363     """
364     timestamp = timestamp + random.randint(100,9999)
365     return timestamp + NTP.NTP_DELTA
366
```

II. MINIMISATION

Code initial

```
179 self.leap = unpacked[0] >> 6 & 0x3
180 self.version = unpacked[0] >> 3 & 0x7
181 self.mode = unpacked[0] & 0x7
182 self.stratum = unpacked[1]
183 self.poll = unpacked[2]
184 self.precision = unpacked[3]
185 self.root_delay = float(unpacked[4])/2**16
186 self.root_dispersion = float(unpacked[5])/2**16
187 self.ref_id = unpacked[6]
188 self.ref_timestamp = _to_time(unpacked[7], unpacked[8])
189 self.orig_timestamp = _to_time(unpacked[9], unpacked[10])
190 self.recv_timestamp = _to_time(unpacked[11], unpacked[12])
191 self.tx_timestamp = _to_time(unpacked[13], unpacked[14])
```

Code modifié

```
179 self.leap = unpacked[0] >> 6 & 0x3
180 self.version = unpacked[0] >> 3 & 0x7
181 self.mode = unpacked[0] & 0x7
182 self.stratum = unpacked[1]
183 self.poll = unpacked[2]
184 #self.poll = unpacked[2]
185 self.precision = unpacked[3]
186 self.root_delay = float(unpacked[4])/2**16
187 self.root_dispersion = float(unpacked[5])/2**16
188 self.ref_id = unpacked[6]
189 self.ref_timestamp = _to_time(unpacked[7], unpacked[8])
190 self.orig_timestamp = _to_time(unpacked[9], unpacked[10])
191 self.recv_timestamp = _to_time(unpacked[11], unpacked[12])
192 self.tx_timestamp = _to_time(unpacked[13], unpacked[14])
```

CAPTURE DES TRAMES 1/2

WHIRESHARK

```
Network Time Protocol (NTP Version 2, client)
> Flags: 0x13, Leap Indicator: no warning, Version number: NTP Version 2, Mode: client
Peer Clock Stratum: unspecified or invalid (0)
Peer Polling Interval: invalid (0)
Peer Clock Precision: 1.000000 sec
Root Delay: 0 seconds
Root Dispersion: 0 seconds
Reference ID: NULL
Reference Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Origin Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Receive Timestamp: Jan 1, 1970 00:00:00.000000000 UTC
Transmit Timestamp: May 11, 2018 09:52:07.539994239 UTC
```

HEURE SYSTEME

```
root@Serveur:~/ntplib# date
jeudi 10 mai 2018, 12:38:24 (UTC+0000)
root@Serveur:~/ntplib# █
```

CAPTURE DES TRAMES 2/2

Initialement

```
Network Time Protocol (NTP Version 2, client)
  > Flags: 0x13, Leap Indicator: no warning, Version number: NTP Version 2, Mode: client
  Peer Clock Stratum: unspecified or invalid (0)
  Peer Polling Interval: 6 (64 sec)
  Peer Clock Precision: 1.000000 sec
  Root Delay: 0 seconds
  Root Dispersion: 0 seconds
```

Après modification

```
Network Time Protocol (NTP Version 2, client)
  > Flags: 0x13, Leap Indicator: no warning, Version number: NTP Version 2, Mode: client
  Peer Clock Stratum: unspecified or invalid (0)
  Peer Polling Interval: invalid (0)
  Peer Clock Precision: 1.000000 sec
  Root Delay: 0 seconds
```



MERCI DE VOTRE AIMABLE ATTENTION