ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

# L'analyse réseau

· L'analyse réseau



ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

# L'analyse réseau

· L'analyse réseau

Qu'est ce que l'analyse réseau?





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

Objectifs:





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

 Déterminer les échanges effectués par l'application





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

- Déterminer les échanges effectués par l'application
- ► Lire le traffic http





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

- Déterminer les échanges effectués par l'application
- ► Lire le traffic http
- Déchiffrer le traffic https

#### Environnement utilisé



1/2

ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

- Déterminer les échanges effectués par l'application
- ► Lire le traffic http
- Déchiffrer le traffic https

#### Environnement utilisé

Emulateur genymotion avec ProxyDroid





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

- Déterminer les échanges effectués par l'application
- ► Lire le traffic http
- ▶ Déchiffrer le traffic https

#### Environnement utilisé

- Emulateur genymotion avec ProxyDroid
- WireShark (Analyseur de paquet)





ntercepter le traffic entrant et sortant de l'ap-

plication, pour détermier quisont les destinataires et comment sont échangés les messages

## L'analyse réseau

· L'analyse réseau

## Qu'est ce que l'analyse réseau?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

### Objectifs:

- Déterminer les échanges effectués par l'application
- ► Lire le traffic http
- ▶ Déchiffrer le traffic https

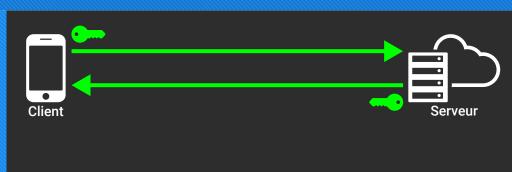
#### Environnement utilisé

- Emulateur genymotion avec ProxyDroid
- WireShark (Analyseur de paquet)
- Xposed : JustTrustMe





# L'analyse réseau : Principe



· L'analyse réseau

# L'analyse réseau : Principe







# L'analyse réseau : Principe

- L'analyse réseau

Client

MITM

Serveur

WIRESHARK