

Analyse réseau :

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

L'analyse réseau

• L'analyse réseau



Analyse réseau :

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

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?



Analyse réseau :

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

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

- ▶ Déterminer les échanges effectués par l'application



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

- ▶ Déterminer les échanges effectués par l'application
- ▶ Lire le trafic http



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

Analyse réseau :

- Emulateur avec ProxyDroid : modifie les règles iptables pour s'assurer que l'application passe forcément par le proxy
- Wireshark pour analyser les paquets interceptés
- JustTrustMe pour désactiver la vérification des certificats SSL/TLS

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

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

Environnement utilisé



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

Analyse réseau :

- Emulateur avec ProxyDroid : modifie les règles iptables pour s'assurer que l'application passe forcément par le proxy
- Wireshark pour analyser les paquets interceptés
- JustTrustMe pour désactiver la vérification des certificats SSL/TLS

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

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

Environnement utilisé

- ▶ Emulateur genymotion avec ProxyDroid



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

Analyse réseau :

- Emulateur avec ProxyDroid : modifie les règles iptables pour s'assurer que l'application passe forcément par le proxy
- Wireshark pour analyser les paquets interceptés
- JustTrustMe pour désactiver la vérification des certificats SSL/TLS

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

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

Environnement utilisé

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



Analyse réseau :

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

Objectifs :

- Déterminer les serveurs avec qui l'application échange
- Traffic http : intercepter et lire les échanges
- Traffic https : intercepter, déchiffrer et lire

Analyse réseau :

- Emulateur avec ProxyDroid : modifie les règles iptables pour s'assurer que l'application passe forcément par le proxy
- Wireshark pour analyser les paquets interceptés
- JustTrustMe pour désactiver la vérification des certificats SSL/TLS

L'analyse réseau

• L'analyse réseau

Qu'est ce que l'analyse réseau ?

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

Objectifs :

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

Environnement utilisé

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



Client-serveur :

- Les échanges sont chiffrés
- Un certificat permet de s'assurer que le serveur est bien celui que l'on attend

MITM :

- Déchiffrer les échanges réalisés
- JustTrustMe pour empêcher la vérification des certificats
- Récupération des données pour être analysées

L'analyse réseau : Principe

• L'analyse réseau



FIGURE – Principe d'une attaque man-in-the-middle

Client-serveur :

- Les échanges sont chiffrés
- Un certificat permet de s'assurer que le serveur est bien celui que l'on attend

MITM :

- Déchiffrer les échanges réalisés
- JustTrustMe pour empêcher la vérification des certificats
- Récupération des données pour être analysées

L'analyse réseau : Principe

• L'analyse réseau



FIGURE – Principe d'une attaque man-in-the-middle

Client-serveur :

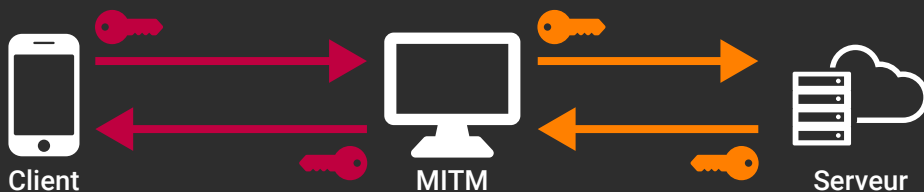
- Les échanges sont chiffrés
- Un certificat permet de s'assurer que le serveur est bien celui que l'on attend

MITM :

- Déchiffrer les échanges réalisés
- JustTrustMe pour empêcher la vérification des certificats
- Récupération des données pour être analysées

L'analyse réseau : Principe

• L'analyse réseau



WIRESHARK

FIGURE – Principe d'une attaque man-in-the-middle