Anàlisi de Tràfic de Xarxa Generat per Aplicacions Android amb Android-x86

**Objectiu**

Capturar i analitzar el tràfic de xarxa generat per aplicacions Android en un dispositiu emulat amb Android-x86 per identificar connexions no segures o comportaments sospitosos.

**Requisits previs**

1. Android-x86 instal·lat i configurat en una màquina virtual.
2. Accés a una eina d’anàlisi de tràfic, com **Wireshark** o **mitmproxy**, instal·lada al sistema host.
3. Una aplicació instal·lada a Android-x86 que necessiti accés a Internet.

**Pas 1: Configura un entorn de captura de tràfic**

Crea un punt d'accés Wi-Fi controlat:

* Configura el teu sistema host per crear un punt d'accés Wi-Fi o utilitza una xarxa NAT a VirtualBox amb redirecció de ports.
* Si utilitzes mitmproxy, pots executar-lo com a intermediari entre Android-x86 i la xarxa:
* mitmproxy --mode transparent

Configura Android-x86 per utilitzar el proxy:

* Ves a **Configuració** > **Wi-Fi**.
* Selecciona la xarxa activa i edita’n les configuracions:
	+ Configura manualment el proxy introduint l’adreça IP del sistema host i el port de l’eina (per exemple, 8080 per mitmproxy).
* Desa els canvis.

**Pas 2: Instal·la i obre una aplicació Android**

Descarrega i instal·la una aplicació APK manualment (des de fonts com APKMirror) o des d’una botiga d’aplicacions.
Inicia l’aplicació i realitza accions que generin tràfic de xarxa, com registrar-se o accedir a contingut.

**Pas 3: Captura el tràfic**

Obre Wireshark o mitmproxy al sistema host:

* Selecciona l’adaptador de xarxa associat a la màquina virtual.
* Filtra el tràfic HTTP o HTTPS utilitzant:
	+ Wireshark: http || tls
	+ mitmproxy: El tràfic es mostrarà directament. Observa el tràfic generat per l’aplicació:
* Identifica sol·licituds HTTP no xifrades.
* Analitza les connexions HTTPS per veure si s’està utilitzant xifrat correcte.
* Busca dades sensibles enviades en text pla, com noms d’usuari o contrasenyes.