TEST TECHNIQUE PRADEO - LÉO BRUNET

- Réaliser une documentation permettant de répondre au deux points suivants :
• Le protocole à suivre pour réaliser une attaque de type ARP Poisoning sur le téléphone

Le protocole à suivre pour réaliser une attaque de type ARP Poisoning sur un téléphone consiste à suivre les étapes suivantes :

- Préparer l'environnement : il est recommandé de disposer d'un ordinateur avec une interface réseau, d'un téléphone mobile et d'une connexion réseau fiable.
- Identifier les cibles : l'attaque de type ARP Poisoning cible généralement les appareils connectés au réseau local. Pour cela, il est nécessaire de trouver l'adresse IP et l'adresse MAC de chaque appareil connecté au réseau.
- Configurer l'ordinateur : il est nécessaire de configurer l'ordinateur en mode "promiscuous", c'est-à-dire en mode de réception de tous les paquets réseau qui traversent l'interface réseau.
- Envoyer des paquets de type ARP : l'attaque consiste à envoyer des paquets de type ARP à chaque appareil cible. Ces paquets contiennent une fausse adresse MAC associée à l'adresse IP de l'ordinateur.
- Surveiller le trafic réseau : une fois que les paquets ARP ont été envoyés, il est recommandé de surveiller le trafic réseau pour vérifier que l'attaque a bien été réalisée avec succès.

• L'algorithme qui permettrait de détecter depuis votre application une attaque ARP Poisoning ciblant le téléphone

Pour détecter une attaque de type ARP Poisoning depuis une application, il est possible d'utiliser l'algorithme suivant :

```
import java.net.NetworkInterface
import java.util.Collections

fun detectArpPoisoning(interfaceName: String) {
  try {
    val networkInterface = NetworkInterface.getByName(interfaceName)
    val arpTable = networkInterface.getArpTable()

    for (arpEntry in arpTable) {
      val targetHardwareAddress = arpEntry.getHardwareAddress()
      val targetProtocolAddress = arpEntry.getProtocolAddress()

      if (targetHardwareAddress != arpEntry.getHardwareAddress()) {
        // L'adresse MAC de l'hôte cible est différente de celle qui est enregistrée dans
la table ARP.
        // Possible attaque ARP Poisoning.
        // Prenez des mesures pour contrer cette attaque.
      }
    }
  } catch (e: Exception) {
    // Gérez les exceptions ici
  }
}
```

Explication de l’algorithme

On commence par **importer les bibliothèques** de réseau nécessaires, telles que java.net et java.util.
On **crée ensuite l’objet NetworkInterface** qui représente l'interface réseau du téléphone en utilisant la méthode NetworkInterface.getByName().
Puis **on récupère la table ARP** du téléphone en utilisant la méthode NetworkInterface.getArpTable().
On parcourt chaque entrée de la table ARP et **on vérifie si l'adresse MAC de l'hôte cible est différente de celle qui est enregistrée dans la table ARP**. Si c'est le cas, cela peut être un signe d'une attaque de type ARP Poisoning.
Si une telle attaque est détectée, il faut prendre des mesures pour la contrer, telles que mettre à jour la table ARP avec l'adresse MAC correcte ou ignorer toutes les communications avec l'hôte cible jusqu'à ce que l'attaque soit résolue.