ATTAQUES ET VULNÉRABILITÉS

ATTAQUES RÉSEAU

MAN IN THE MIDDLE

- MiTM : « homme du milieu »
- Désigne tout type d’attaque dans laquelle une transmission est intercepté, voire modifiée
- L’attaquant « s’insère » dans la conversation entre les deux parties communiquantes
- Ces deux parties n’ont pas conscience de l’attaque

ATTAQUE WI-FI - JAMMING

- Envoi de signaux de bruit excessif sur les fréquences Wi-Fi, rendant les canaux Wi-Fi impraticables
- Requiert un équipement spécifique (souvent de fabrication-maison)

WI-FI - POINT D’ACCÈS PIRATE

- Attaque de type MiTM
- Mise en place d’un point d’accès Wi-Fi non-autorisé (*rogue*) dans l’organisation (ou à proximité)
  - vol ou altération de données
  - peut être combiné avec une attaque de *jamming*/interférence pour brouiller les points d’accès légitimes

VARIATION - JUMEAU MALVEILLANT (EVIL TWIN)

- Point d’accès *rogue* qui se fait passer pour légitime
  - utilisation du même SSID
- Peut se « déguiser » en portail captif malveillant : imite le portail captif légitime de l’organisation pour récupérer des identifiants de connexion

BLUEJACKING

- Envoi de messages / données à l’appareil victime via la technologie Bluetooth
- Typiquement une vCard contenant un message dans le champ nom par l’intermédiaire du protocole OBEX (*OBjectEXchange*)
  - l’appareil cible doit avoir son module Bluetooth activé en mode découverte
  - proximité nécessaire
- Pas de danger réel, principalement utilisé en tant que « jeu »

BLUESNARFING

- Inverse du *Bluejacking* : cette fois les données sont extraites depuis l’appareil cible
  - liste de contacts, photos, messages, emails…
- Il faut donc intégrer les vulnérabilités associées à la technologie Bluetooth dans la politique de sécurité de l’organisation
- D’autres technologies (NFC) peuvent également être vulnérables à des attaque de proximité

DISSOCIATION

- Création d’un scénario de type Déni de Service (*DoS*) sur un réseau sans fil
- Technique : envoi de frame de dissociation *spoofée* sur le point d’accès
  - Le point d’accès pense que l’appareil s’est dé-authentifié et le déconnecte

DISSOCIATION AVEC AIRCRACK-NG

- Aircrack-ng est une suite d’utilitaires pour tester un réseau Wi-Fi
- Aireplay-ng est l’utilitaire qui permet d’injecter des frames dans les transmissions

AIREPLAY-NG - EXEMPLE

```
$ aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AE:CE:9D ath0
```

- `-0` : code pour la dé-authentification
- `1` : nombre de dé-authentification à envoyer
- `-a adresse_MAC` : adresse du point d'accès
- `-c adresse_MAC` : adresse du client à dé-authentifier
- `ath0` : nom de l'interface réseau

STANDARDS DE CHIFFREMENT WI-FI

- Les standards :
  - WEP
  - WPA
  - WPA2
  - WPA3

ATTAQUES DE VECTEUR D'INITIALISATION (VI)

- Un vecteur d'initialisation est une séquence de bits envoyée avec le premier bloc de données dans un envoi chiffré
- Certains protocoles de chiffrement plus faibles ont des IV courts se répétant fréquemment
  - ex : WEP, IV de 24 bits - en sniffant suffisamment de paquets Wi-Fi, on peut trouver cette IV et obtenir un accès

STANDARDS PLUS SÛRS

- WPA-TKIP est une évolution de WEP mais des vulnérabilités existent également ⇒ à éviter si possible
- WPA2 (AES-CCMP) est considéré comme sûr
- WPA3 n’a pas encore été adopté largement

MAN IN THE BROWSER

- Un malware (de type cheval de Troie) est installé sur la machine cible
  - s’exécute avec le navigateur (extension, JavaScript ou autre mécanisme)
  - quand un site connu vulnérable est visité, le malware agit en tant qu’entité MiTM et capture / détourne / modifie les données
- Le milieu bancaire considère ce type d’attaque comme l’une des ses toutes premières menaces

EMPOISONNEMENT ARP

- Plus précisément : empoisonnement du **cache** ARP
- Aussi appelé *ARP Spoofing*
- ARP : *Address Resolution Protocol*
  - au sein d'un réseau, permet : adresse IP ⇒ adresse MAC

EMPOISONNEMENT ARP - TECHNIQUE

- L’attaquant A envoie de faux messages ARP qui communiquent aux autres machines du LAN sa propre adresse MAC associée à l’IP d’une machine M du réseau
  - lorsqu’une machine veut communiquer avec M dont elle connaît l’IP, elle envoie en réalité son message à A
  - particulièrement efficace si on se fait passer pour une passerelle

USURPATION D’ADRESSE IP

- *IP Spoofing*
- Fait de modifier son adresse IP source
- Il est également possible de spoofer une adresse MAC

DDOS

- *Distributed Denial of Service* (attaque en déni de service distribuée)
- Attaque de grande ampleur (nécessite une grande puissance)