BTS SIO2 CYBERSECURITE SLAM DATE:06-11-2023

CHAPITRE 4 : LES ATTAQUES INFORMATIQUES

SOMMAIRE :

- Définitions
- Les types d'attaques
- Les attaques réseaux
  - Les attaques contre le contrôle d'accès
  - Les attaques contre la confidentialité
  - Les attaques contre l'intégrité
  - Les attaques contre l'authentification
  - Les attaques contre la disponibilité
- Documents recommandés
- TD 2
- TD 3
- Corrigé TD 2
- Corrigé TD 3
- TP 1 - Installation et configuration du Snort sur Kali Linux

CHAPITRE 4 : LES ATTAQUES INFORMATIQUES

Définition:

Une cyberattaque désigne un effort intentionnel visant à voler, exposer, modifier, désactiver ou détruire des données, des applications ou d'autres actifs ou à obtenir un accès non autorisé.

- **Internet Engineering Task Force définit l'attaque dans RFC 2828 comme :**

« Un assaut sur la sécurité du système qui découle d'une menace intelligente, c'est-à-dire d'un acte intelligent qui est une tentative délibérée (en particulier dans le sens d'une méthode ou d'une technique) pour échapper aux services de sécurité et violer la politique de sécurité d'un système. »

- Le gouvernement des États-Unis, selon l'instruction CNSS n°4009 du 26 avril 2010 par le Comité des systèmes de sécurité nationale des États-Unis d'Amérique définit une attaque comme suit :

« Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même. »

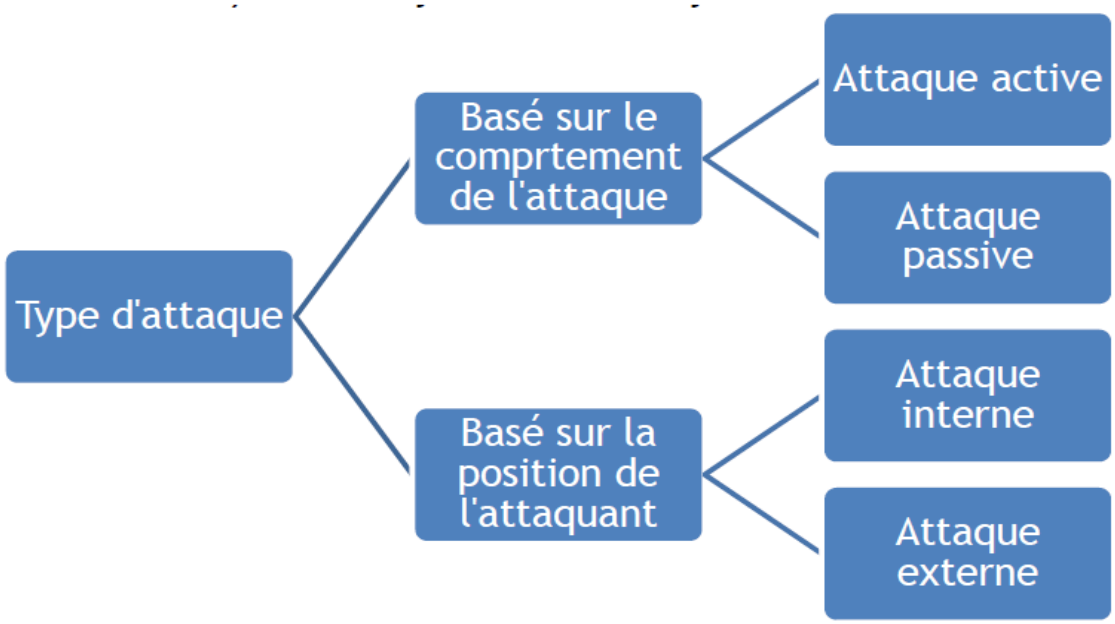


Figure 2.1 Les types d'attaques

2.2. Les types d'attaques

Comme présenté dans la Figure 2.1, une attaque peut être classée par son comportement ou par la position de l'attaquant. Une attaque peut être active ou passive.

• Une **«attaque active»** tente de modifier les ressources du système ou d'affecter leur fonctionnement.
• Une **«attaque passive»** tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).
Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'organisation.
• Une **«attaque interne»** est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui lui ont accordé l'autorisation.
• Une **«attaque extérieure»** est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.

2.3. Les attaques réseaux

Les attaques réseaux contre 802.11 et 802.1X, peuvent être classées selon le type de menace, et mises en correspondance avec des méthodes et des outils de piratage associés, à savoir, les attaques contre le contrôle d'accès, les attaques contre la confidentialité, les attaques contre l'intégrité, les attaques contre l'authentification, et les attaques contre la disponibilité, comme présenté dans la Figure 2.22.

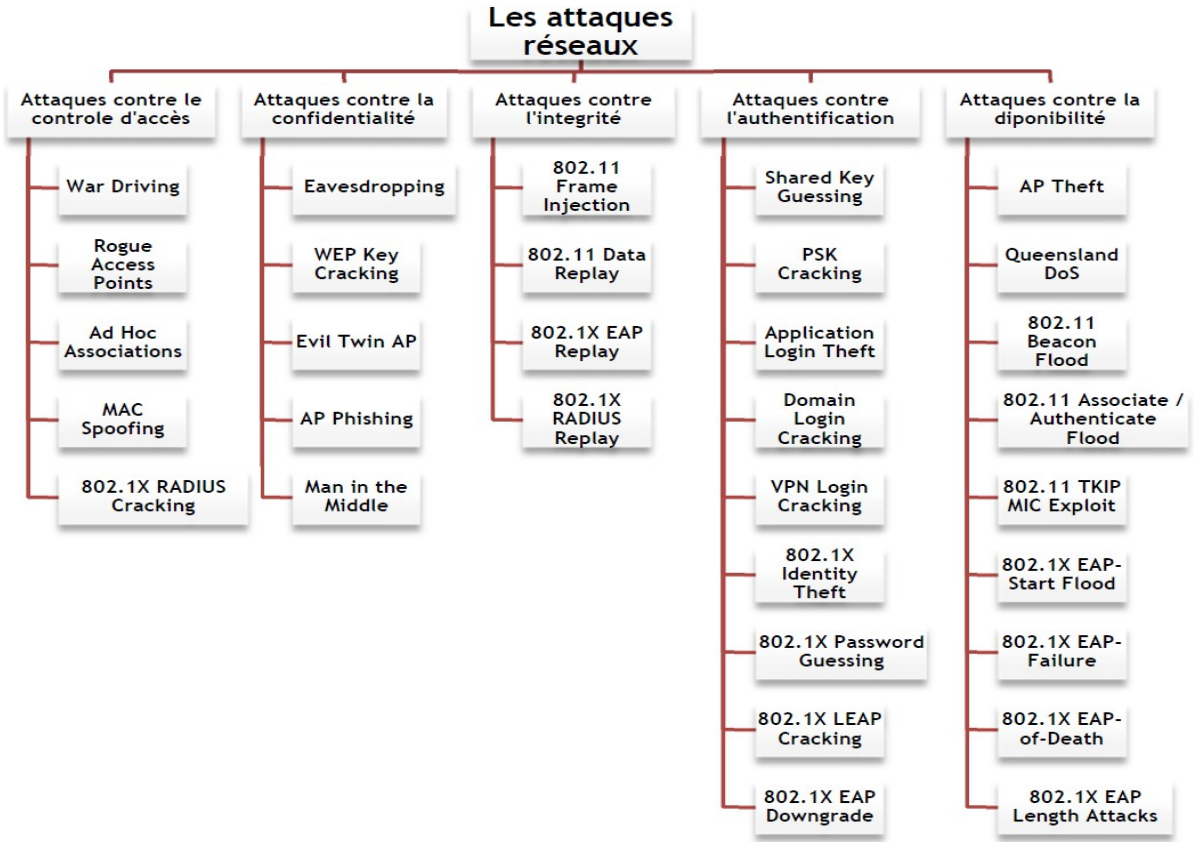


Figure 2.2 Les attaques réseaux

2.3.1. Attaques contre le contrôle d'accès

Ces attaques tentent de pénétrer dans un réseau en utilisant des mesures de contrôle d'accès WLAN sans fil, comme les filtres AP MAC et les contrôles d'accès au port 802.1X. (Voir la liste des attaques dans le Tableau 2.1.)

Type d'attaque	Description	Méthodes et outils
War Driving	Découvrir les réseaux locaux sans fil en écoutant des balises ou en envoyant des requêtes de sonde, fournissant ainsi un point de lancement pour d'autres attaques.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Installation d'un point d'accès non sécurisé dans un pare-feu, création d'une porte dérobée ouverte dans un réseau de confiance.	Tout point d'accès matériel ou logiciel
Ad Hoc Associations	Connexion directe à une station non sécurisée pour contourner la sécurité de l'AP ou la station d'attaque.	Toute carte sans fil ou adaptateur USB
MAC Spoofing	Reconfiguration de l'adresse MAC d'un attaquant pour se présenter comme un AP ou une station autorisée.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X.	Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS

Tableau 2.1 les attaques contre le contrôle d'accès

• **L'attaque « War Driving» :** La conduite de guerre, également appelée cartographie des points d'accès, consiste à localiser et éventuellement exploiter des connexions aux réseaux locaux sans fil tout en conduisant autour d'une ville ou ailleurs, comme présenté dans la Figure 2.3. Pour faire une conduite de guerre, vous avez besoin d'un véhicule, d'un ordinateur (qui peut être un ordinateur portable), d'une carte Ethernet sans fil configurée en mode promiscuous et d'une sorte d'antenne qui peut être montée au-dessus ou positionnée à l'intérieur de la voiture. Étant donné qu'un réseau local sans fil peut avoir une portée qui s'étend au-delà d'un immeuble de bureaux, un utilisateur extérieur peut pénétrer le réseau, obtenir une connexion Internet gratuite et accéder éventuellement aux enregistrements de l'entreprise et à d'autres ressources.
Avec une antenne omnidirectionnelle et un système de positionnement géophysique (GPS), le conducteur de guerre peut systématiquement localiser les emplacements des points d'accès sans fil 802.11b. Les

entreprises qui ont un réseau local sans fil sont entrain d'ajouter des garanties de sécurité qui assureront uniquement les utilisateurs visés. Les garanties comprennent l'utilisation de la norme de chiffrement WEP (Wired Equivalent Privacy), Ipsec ou Wi-Fi Protected Access (WPA), avec un pare-feu ou DMZ.

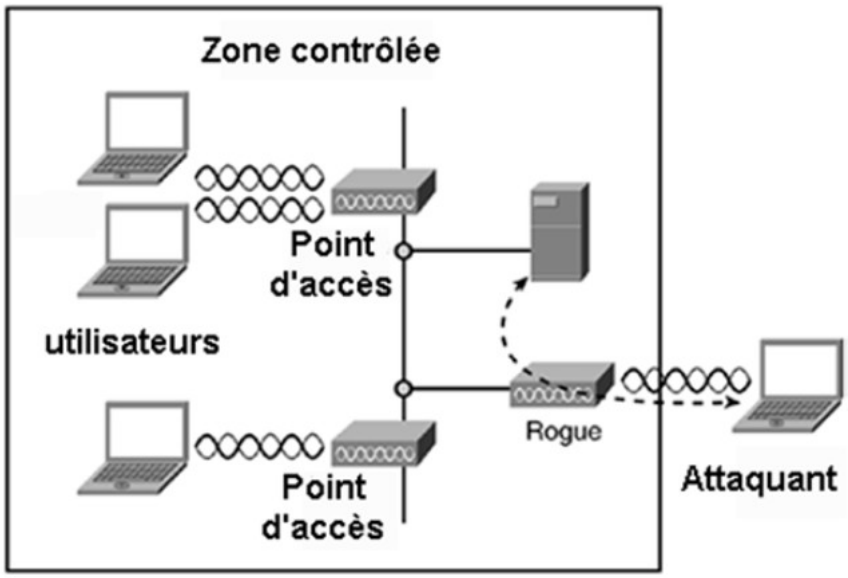
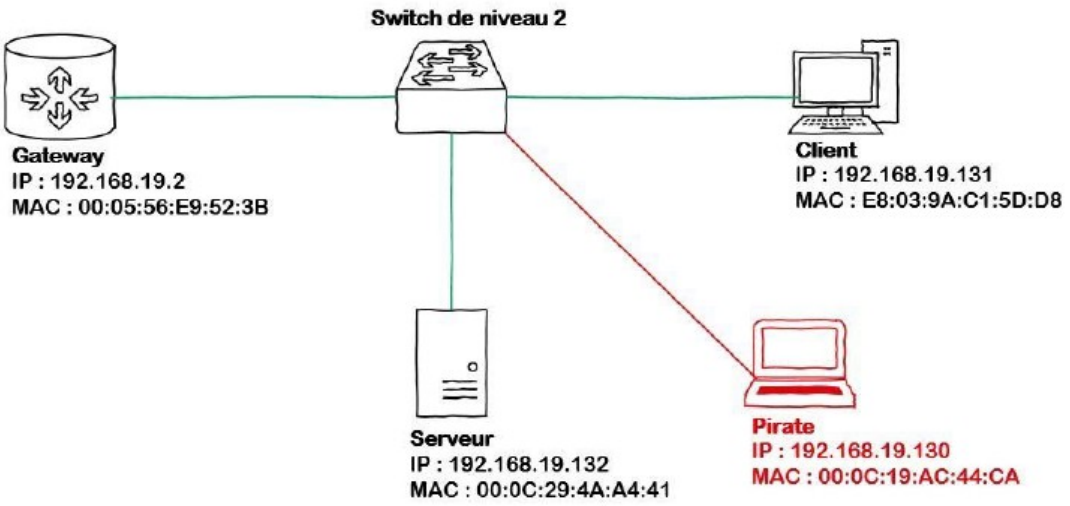


Figure 2.4 L'attaque « Rogue Access Points »

• L'attaque « Rogue Access Points » : Cette attaque se base sur l'installation d'un point d'accès non sécurisé dans un pare-feu, puis la création d'une porte dérobée ouverte dans un réseau de confiance, comme présenté dans la Figure 2.4. Les grandes entreprises investissent souvent dans des systèmes de prévention des intrusions sans fil (WIPS) qui utilisent des capteurs distribués pour surveiller à plein temps le trafic sans fil.

• L'attaque « Ad Hoc Associations » : Les réseaux ad hoc ne sont pas sans risques. Probablement le plus grand risque associé à la mise en réseau ad hoc a toujours été l'écoute électronique. Traditionnellement, les connexions ad hoc ont manqué les différents mécanismes de cryptage qui sont habituellement utilisés avec des points d'accès sans fil tels que WEP et WPA.



• L’attaque « MAC Spoofing »: La falsification MAC est une technique permettant de modifier une adresse de contrôle d'accès aux médias (MAC) attribuée à une interface réseau sur un périphérique en réseau. L'adresse MAC codée sur un contrôleur d'interface réseau (NIC) ne peut pas être modifiée. Cependant, de nombreux pilotes permettent de modifier l'adresse MAC. De plus, il existe des outils qui permettent à un système d'exploitation de croire que la NIC a l'adresse MAC du choix d'un utilisateur. Le processus de masquage d'une adresse MAC est connu sous le nom de spoofing MAC. Essentiellement, la spoofing MAC implique de changer l'identité d'un ordinateur, pour quelque raison que ce soit, et c'est relativement facile. Comme présenté dans la Figure 2.5, le changement de l'adresse MAC assignée peut permettre de contourner les listes de contrôle d'accès sur les serveurs ou les routeurs, soit en cachant un ordinateur sur un réseau, soit en la permettant d'imiter un autre périphérique réseau. La falsification MAC est effectuée à des fins légitimes et illicites.
• L’attaque « 802.1X RADIUS Cracking » : Cette attaque se base sur la récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X. De plus, cette attaque peut être lancée par un Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS

2.3.2. Attaques contre la confidentialité :

Ces attaques tentent d'intercepter des informations privées envoyées sur des associations sans fil, soit envoyé en clair ou chiffré par 802.11 ou des protocoles de couche supérieure. (Voir la liste des attaques dans le Tableau 2.2)

Type d'attaque	Description	Méthodes et outils
Eavesdropping (Ecoute)	Capture et décodage du trafic d'application non protégé pour obtenir des informations potentiellement sensibles.	bsd-airtools, Ettercap, Kismet, Wireshark
WEP Key Cracking	Capture de données pour récupérer une clé WEP en utilisant des méthodes passives ou actives.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	Masquage en tant qu'appareil autorisé en balayant l'identificateur du WLAN (SSID) pour attirer les utilisateurs.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Exécution d'un faux portail ou d'un serveur Web sur un AP double mal à "phish" pour les connexions d'utilisateurs, les numéros de carte de crédit.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle (d'attaque de l'homme dans le milieu)	Exécuter des outils traditionnels d'attaque de l'homme dans le milieu pour intercepter des sessions TCP ou des tunnels SSL / SSH.	dsniff, Ettercap-NG, sshmitm

Tableau 2.2 les attaques contre la confidentialité

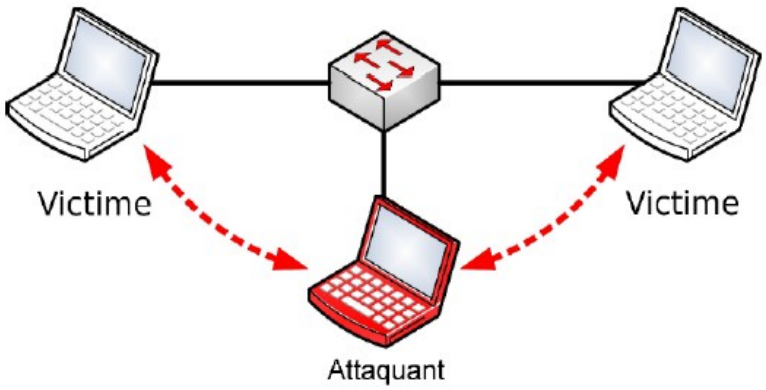


Figure 2.6 L'attaque Eavesdropping

• L'attaque « Eavesdropping - Ecoute» : présenté dans la Figure 2.6, se base sur l'interception non autorisée en temps réel d'une communication privée, comme un appel téléphonique, un message instantané, une vidéoconférence ou une transmission de télécopie. Le terme «écoute» dérive de la pratique de se tenir debout sous les avant-toits d'une maison, en écoutant des conversations à l'intérieur.

• L'attaque « WEP Key Cracking » : se base sur la capture de données pour récupérer une clé WEP en utilisant des méthodes passives ou actives. Nous citons les outils suivants pour lancer cette attaque : aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab,

wesside.
• L’attaque «Evil Twin AP» : Un Evil Twin est un faux point d'accès sans fil qui prétend être un AP légitime en annonçant le nom du WLAN (c'est-à-dire l'identificateur de set de service étendu, SSID). Un Evil Twin peut utiliser KARMA, un outil d'attaque qui surveille les sondes de la station, surveille les SSID couramment utilisés et adopte l'un comme son propre. Ou un Evil Twin peut être configuré avec un SSID résidentiel commun (par exemple, linksys), SSID de point d'accès (par exemple, Wayport_Access) ou le SSID d'un WLAN d'une entreprise spécifique. Même les AP qui n'émettent pas de SSID dans les balises peuvent être ciblés, pourvu que les utilisateurs légitimes puissent être surveillés avec Wireshark, Kismet ou un autre analyseur WLAN.
• **L’attaque « AP Phishing » :** se base sur l'exécution d'un faux portail ou d'un serveur Web sur un AP double mal à "phish" pour les connexions d'utilisateurs, les numéros de carte de crédit. Les outils suivants peuvent être utilisés pour lancer cette attaque : Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP.

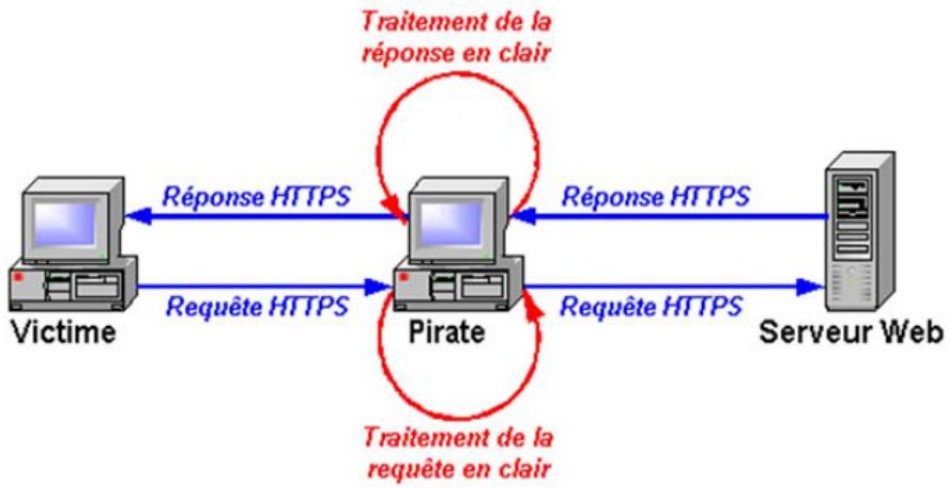


Figure 2.7 L’attaque Man in the Middle
• **L’attaque « Man in the Middle» :** est celle dans laquelle l'attaquant intercepte et relève secrètement les messages entre deux parties qui croient communiquer directement entre elles, comme présenté dans la Figure 2.7.
2.3.3. Attaques contre l’intégrité :
les attaques contre l’intégrité se basent sur l’envoi des contrôles forgés, de la gestion ou des trames de données sur un réseau sans fil pour induire le destinataire ou faciliter un autre type d'attaque (par exemple, l'attaque DoS). (Voir la liste des attaques dans le Tableau 2.4)

Type d'attaque	Description	Méthodes et outils
802.11 Frame Injection	Création et envoi des trames forgées 802.11.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capture des trames de données 802.11 pour une relecture ultérieure (modifiée).	Capture + Outils d'injection
802.1X EAP Replay	Capture des protocoles d'authentification extensible 802.1X pour une relecture ultérieure.	Capture sans fil + Outils d'injection entre une station et l'AP
802.1X RADIUS Replay	Capture d'accès RADIUS: accepter ou rejeter les messages pour une nouvelle version ultérieure.	Ethernet Capture + Injection Tools between AP and authentication server

Tableau 2.3 les attaques contre l'intégrité

2.3.4. Attaques contre l'authentification :

Les attaquants contre l'authentification utilisent ces attaques pour voler les identités et les informations d'identification des utilisateurs légitimes pour accéder aux réseaux et services privés. (Voir la liste des attaques dans le Tableau 2.4)

Type d'attaque	Description	Méthodes et outils
Shared Key Guessing	Tentative d'authentification de clé partagée 802.11 avec des clés WEP supposées et craquées.	WEP Cracking Tools
PSK Cracking	Récupération d'un PSPA / WPA2 PSK à partir de trames clés de handshake capturés en utilisant un outil d'attaque de dictionnaire.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capture des informations d'identification des utilisateurs (par exemple, adresse e-mail et mot de passe) à partir des protocoles d'application en clair.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, connexion et mot de passe du Windows) en crachant les hachages de mot de passe NetBIOS en utilisant un outil d'attaque de force brute ou de dictionnaire.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, le mot de passe PPTP ou la clé Secret pré-partagé IPsec) en exécutant des attaques de force brute sur les protocoles d'authentification VPN.	ike_scan et ike_crack (IPsec), anger et THC-pptp-bruter (PPTP)
802.1X Identity Theft	Capture d'identité des utilisateurs à partir de paquets de réponse	Capture Tools
802.1X Password Guessing	Utilisation d'une identité capturée, tentative répétée d'authentification 802.1X pour deviner le mot de passe de l'utilisateur.	Password Dictionary
802.1X LEAP Cracking	Récupération des informations d'identification des utilisateurs à partir des paquets légers EAP (LEAP) 802.1X capturés à l'aide d'un outil d'attaque de dictionnaire pour déchiffrer le hash du mot de passe NT.	Anwrap, Asleap, THC-LEAPcracker
802.1X EAP Downgrade	Forcer un serveur 802.1X à offrir un type d'authentification plus faible en utilisant des paquets forés EAP.	File2air, libradiate

Tableau 2.4 les attaques contre l'authentification

2.3.5. Attaques contre la disponibilité :

Ces attaques empêchent la livraison de services sans fil à des utilisateurs légitimes, soit en leur refusant l'accès aux ressources WLAN, soit en paralysant ces ressources. (Voir la liste des attaques dans le Tableau 2.5)

Attaque	Description	Outils
AP Theft	Suppression physique d'un AP d'un espace public.	"Five finger discount"
Queensland DoS	Exploiter le mécanisme d'évaluation des canaux clairs (CCA) CSMA / CA pour que le canal apparaisse occupé.	Un adaptateur prenant en charge le mode CW Tx, avec un utilitaire de bas niveau pour invoquer une transmission continue
802.11 Beacon Flood	Générer des milliers de balises contrefaites 802.11 pour rendre difficile aux stations de trouver un AP légitime.	FakeAP
802.11 Associate / Authenticate Flood	Remplir le tableau d'association d'AP cible.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Générer des données TKIP non valides pour dépasser le seuil d'erreur MIC cible AP pour suspendre le service WLAN.	File2air, wnet dinject, LORCON
802.1X EAP-Start Flood	Inondant un AP pour consommer des ressources ou bloquer la cible.	QACafe, File2air, libradiate
802.1X EAP-Failure	En observant un échange EAP 802.1X valide, puis en envoyant à la station un message falsifié.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Envoi d'une réponse d'identité EAP 802.1X mal formée connue pour provoquer une panne de certains points d'accès.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Envoi de messages spécifiques au type EAP avec des champs de longueur incorrecte pour tenter de bloquer un serveur AP ou RADIUS.	QACafe, File2air, libradiate

Tableau 2.5 les attaques contre la disponibilité