Menaces Réseau, conception de réseau sécurisée.

Table des matières

Table des figures

Chapitre 1

Attaques Fondamentales et Exploitation des Protocoles

1.1 Packet Sniffing et Spoofing

1.1.1 Packet Sniffing (Écoute de Paquets)

C'est le processus d'interception et d'enregistrement du trafic passant sur un réseau. Le cœur du sniffing réside dans le mode promiscueux (ou promiscuous mode).

- Mode Normal : Par défaut, lorsqu'une carte réseau (NIC) reçoit un paquet, elle vérifie l'adresse MAC de destination. Si cette adresse ne correspond pas à la sienne ou à l'adresse de diffusion (broadcast), elle ignore et rejette le paquet au niveau matériel.
- Mode Promiscueux : Lorsqu'il est activé, il ordonne à la carte réseau de capturer absolument tous les paquets qu'elle voit sur le média (câble ou onde), sans tenir compte de l'adresse de destination. La carte transmet alors toutes ces données au système d'exploitation et aux applications de sniffing (comme Wireshark, tcpdump ou scapy) pour analyse.

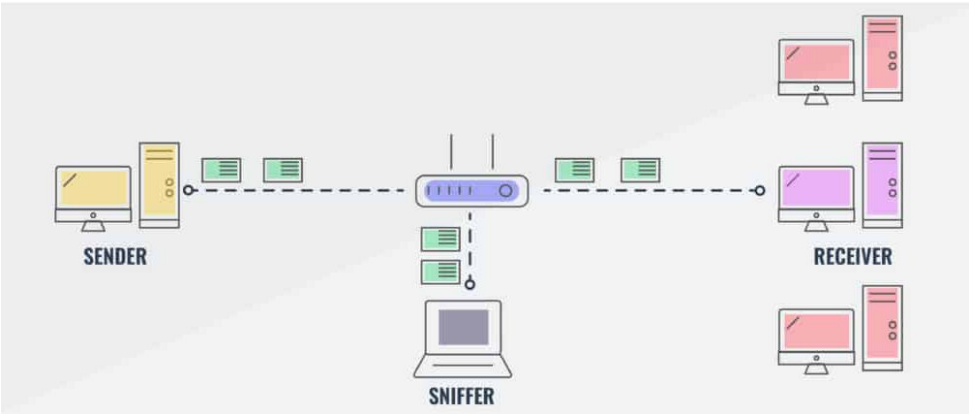

FIGURE 1.1 – Reniflement de packet sur un routeur

1.1.2 Packet Spoofing (Usurpation de Paquets)

L'usurpation consiste à créer des paquets réseau avec une fausse adresse source. L'un des exemples les plus critiques est l'**IP Spoofing**, qui est largement utilisé dans les attaques par déni de service.

L'objectif premier du spoofing dans un contexte de déni de service (DoS) est de masquer la véritable source de l'attaque.

- Si l'attaquant envoie directement tous les paquets avec sa propre adresse IP source, le système de défense de la victime (ou l'opérateur réseau) peut facilement identifier et bloquer cette adresse (via un firewall ou un filtrage au niveau du fournisseur d'accès).
- En utilisant une adresse source aléatoire ou falsifiée pour chaque paquet, l'attaquant empêche toute riposte immédiate et rend la traçabilité (traceback) extrêmement difficile.

1.2 L'Attaque de l'Homme du Milieu (MITM)

1.2.1 ARP Poisoning

Le protocole Address Resolution Protocol (ARP) mappe les adresses IP aux adresses MAC sur un réseau local. L'**ARP Poisoning** exploite la nature non sécurisée d'ARP en envoyant de fausses réponses pour rediriger le trafic vers l'attaquant.

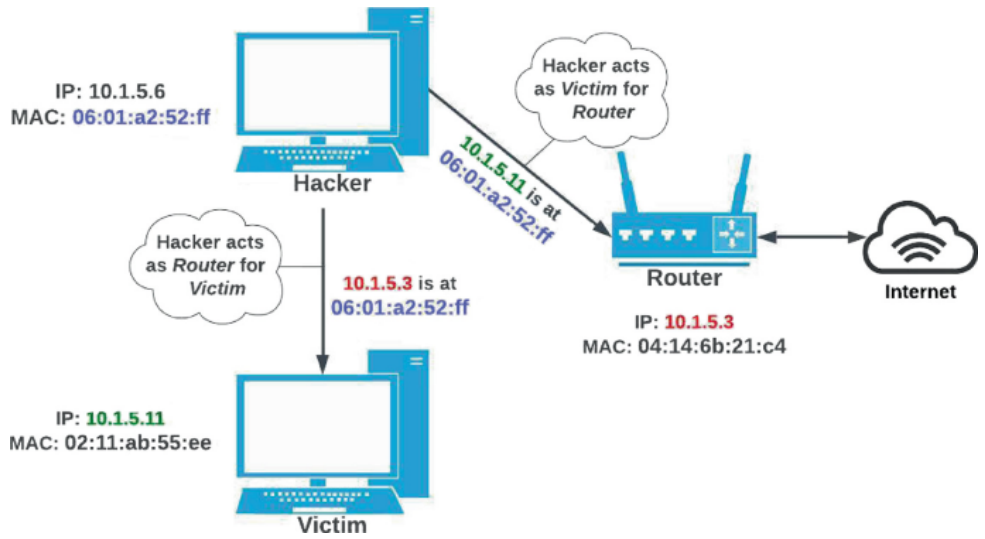

FIGURE 1.2 – Schéma du flux de trafic dans une attaque MITM par ARP Poisoning.

1.2.2 MITM via ARP et Sniffing

Une fois le cache ARP des victimes empoisonné, l'attaquant peut activer le forwarding pour relayer le trafic et s'interposer. Le **packet sniffing** est alors utilisé pour capturer et analyser toutes les données échangées (identifiants, etc.).

Chapitre 2

Solutions et Architectures de Défense

2.1 DMZ (Demilitarized Zone)

La Demilitarized Zone (DMZ) est un sous-réseau physique ou logique qui contient les services orientés vers l'extérieur (serveur Web, FTP, Mail) d'une organisation. Elle agit comme une zone tampon entre le réseau interne (LAN) et Internet, offrant une segmentation cruciale.

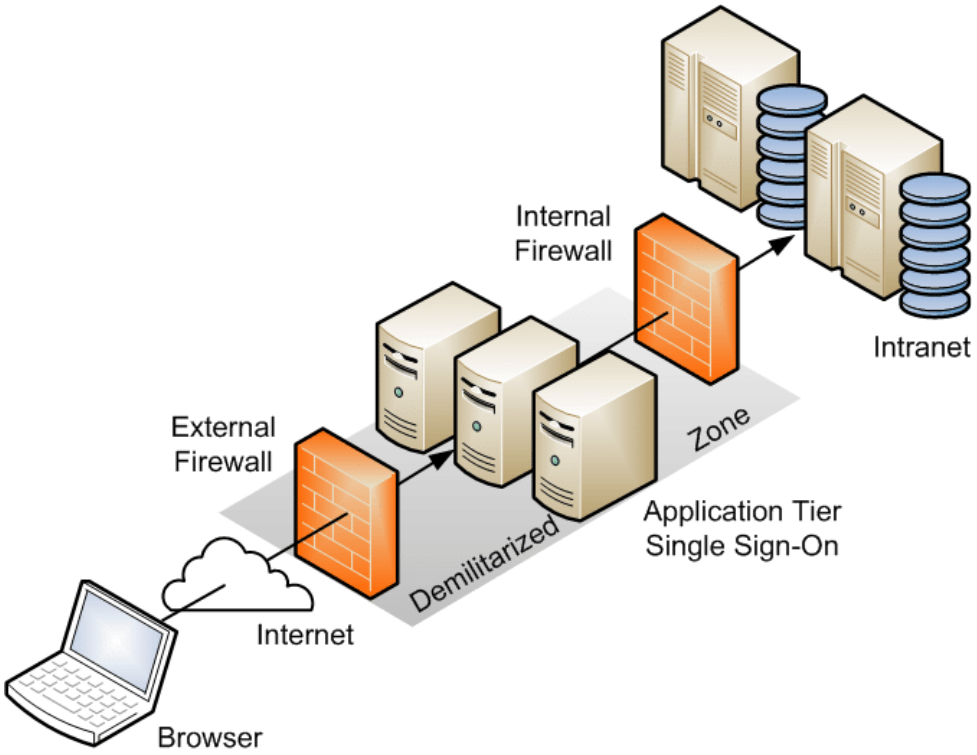

FIGURE 2.1 – Schéma de zone démilitarisée dans un réseau

2.1.1 Avantages du DMZ

Le DMZ peut accomplir deux fonctions simultanément :

- Rupture de Chaîne : Si un attaquant parvient à compromettre un serveur public (comme un serveur web ou un serveur mail), il se retrouve isolé dans la DMZ. Il ne peut pas accéder directement et facilement aux ressources critiques de l'entreprise situées sur le réseau interne (LAN).
- Protection du LAN : Le réseau interne est le point le plus sensible de l'entreprise (données clients, bases de données, postes de travail des employés). La DMZ le sépare d'Internet par un deuxième niveau de pare-feu (dans les architectures les plus sûres), rendant l'accès au LAN beaucoup plus difficile.

2.2 VPN (Virtual Private Network)

Le Virtual Private Network (VPN) crée un tunnel sécurisé et chiffré sur un réseau non sécurisé (Internet). Il est essentiel pour protéger les communications contre le **packet sniffing** sur les réseaux Wi-Fi publics ou pour connecter les employés distants.

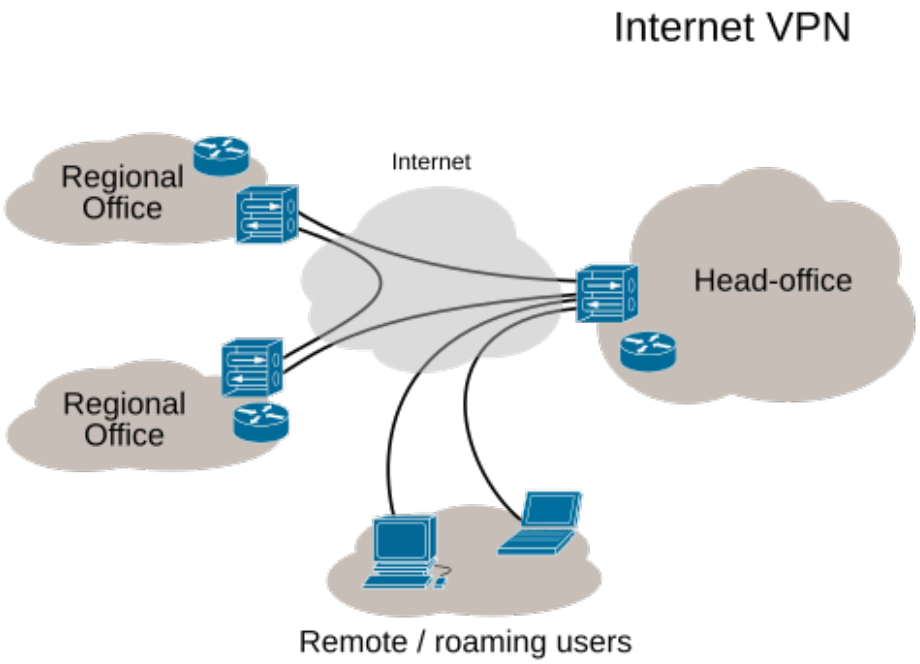

FIGURE 2.2 – Schéma de VPN

Un VPN doit assurer les quatre fonctions suivantes :

1. Authentification - garantir que les données proviennent de la source qu'elles revendiquent.
2. Contrôle d'accès - limiter l'accès des utilisateurs non autorisés au réseau.
3. Confidentialité - Empêcher quiconque de lire les données lorsqu'elles transitent par le réseau.
4. Intégrité des données - Empêcher quiconque d'altérer les données lorsqu'elles transitent par le réseau.

Une passerelle VPN est un dispositif réseau qui fournit un service de chiffrement et d'authentification à une multitude d'hôtes qui s'y connectent.Depuis l'extérieur (Internet), toutes les communications adressées aux hôtes internes passent par la passerelle.

Il existe deux types de tunnels VPN :

1. Ordinateur-à-passerelle (Computer-to-Gateway) - mis en place pour permettre à un utilisateur distant de se connecter au réseau interne de l'entreprise.
2. Passerelle-à-passerelle (Gateway-to-Gateway) réseau d'entreprise à entreprise (par exemple, connecter des succursales de banques entre elles). Dans ce cas, le tunnel est fait entre deux passerelles.

2.2.1 VPN IPsec : Mécanisme d'Encapsulation et de Chiffrement

Le VPN crée un **tunnel sécurisé** entre l'hôte distant et le réseau de l'entreprise, assurant la confidentialité et l'intégrité des données via des protocoles comme **IPsec**. L'exemple ci-dessous illustre le flux de communication en mode tunnel (le plus courant), utilisant l'encapsulation.

Exemple de Communication Chiffrée (IPsec)

Considérons le scénario : un Hôte distant (`1.2.3.4`) veut joindre un Serveur interne (`192.168.1.10`) via un Serveur VPN (`5.6.7.8`).

1. **Attribution d'Adresse Interne :** Le client VPN se connecte et reçoit une adresse IP interne temporaire (`192.168.1.50`).
2. **Encapsulation et Chiffrement (Client vers VPN) :**
   - Le paquet original (`192.168.1.50` → `192.168.1.10`) est **chiffré** (Confidentialité).
   - Ce paquet chiffré devient la **charge utile** d'un nouveau paquet IP (Encapsulation).
   - Ce paquet "extérieur" est adressé à la passerelle publique du VPN.

TABLE 2.1 – En-têtes de Paquets lors de l'envoi (Client → VPN)

Type d'En-tête	Adresse Source	Adresse Destination
Paquet Externe (IPsec)	`1.2.3.4` (Client Public)	`5.6.7.8` (VPN Public)
Paquet Interne (Chiffré)	`192.168.1.50` (Client VPN)	`192.168.1.10` (Serveur)

- **Décapsulation et Routage (Serveur VPN) :**
  - Le serveur VPN reçoit le paquet, vérifie l'intégrité via le **Header de Sécurité** (ESP), puis le **décrypte**.
  - Il route le paquet déchiffré (`192.168.1.50` → `192.168.1.10`) directement vers le réseau interne.
- **Flux de Réponse (Serveur → Client) :** Le processus s'inverse, le serveur VPN chiffrant le paquet de réponse (`192.168.1.10` → `192.168.1.50`) avant de l'encapsuler pour l'envoi via Internet à l'adresse publique du client.

Le Rôle du Header de Sécurité (ESP/AH)

Le protocole **IPsec** s'appuie sur des en-têtes spécifiques pour garantir les services de sécurité.

- **ESP (Encapsulating Security Payload) :** C'est le protocole le plus utilisé pour les VPN. Il assure à la fois la **Confidentialité** (chiffrement) et l'Intégrité/Authentification des données. C'est le mécanisme de chiffrement qui rend le contenu illisible pour les renifleurs de paquets.
- **AH (Authentication Header) :** Assure uniquement l'intégrité et l'authentification. Il garantit que les données n'ont pas été altérées pendant le transit, mais ne fournit pas le chiffrement.

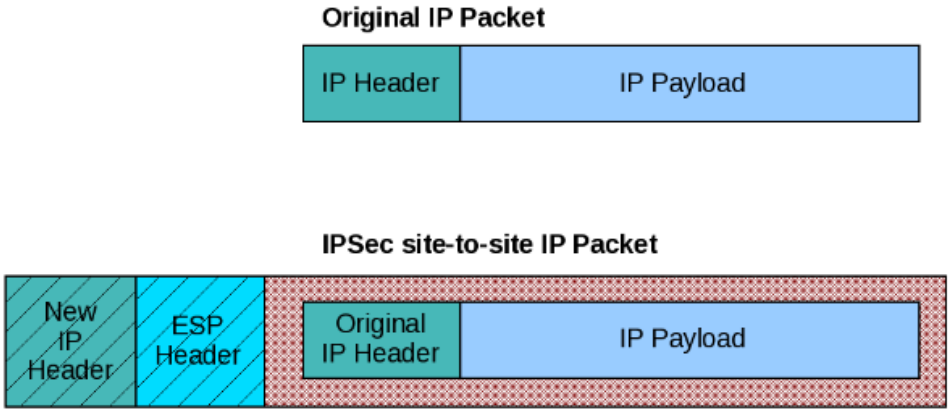

FIGURE 2.3 – Paquet encodé par IPSec

Chapitre 3

Solutions et Architectures de Défense

3.1 Systèmes de Détection et de Prévention d'Intrusion (IDS/IPS)

Les systèmes de détection et de prévention d'intrusion sont cruciaux pour la surveillance en temps réel du trafic réseau, agissant comme des renifleurs avancés.

3.1.1 Distinction IDS vs. IPS

La différence fondamentale réside dans l'action suite à la détection :

- **IDS (Intrusion Detection System)** : Fonctionne en mode passif. Il **détecte** l'activité malveillante et génère des **alertes** (logs, emails).
- **IPS (Intrusion Prevention System)** : Fonctionne en mode actif (inline). Il **détecte et bloque** immédiatement le trafic malveillant. Il est considéré comme plus efficace pour la prévention immédiate.

3.1.2 Attaque/vulnérabilité Zero-day

Une vulnérabilité Zero-Day est une faille de sécurité dans un logiciel qui est inconnue de l'éditeur (le développeur) et, par conséquent, aucun correctif (patch) n'existe pour elle. Le terme "Zero-Day" signifie littéralement :

- Zéro jour d'avertissement pour l'éditeur avant que la faille ne soit exploitée.
- Zéro jour depuis que le correctif est disponible.

3.1.3 Méthodes de Détection

La détection est principalement basée sur deux mécanismes :

- **Détection par Signatures :** Similaire aux antivirus, elle identifie des **éléments distinctifs** d'exploits déjà connus. Cette méthode nécessite des bibliothèques de signatures et des **mises à jour très régulières**. Elle est inefficace contre les attaques Zero-Day (inconnues).
- **Détection par Anomalies :** Le système apprend le **comportement normal** du réseau et génère des alertes lorsque le trafic s'écarte significativement de cette norme. Bien que potentiellement efficace contre les Zero-Day, elle présente un **risque élevé de faux positifs** si la norme est mal définie.

TABLE 3.1 – Comparaison des méthodes de détection

Caractéristique	**Signatures**	**Anomalies**
Mises à jour fréquentes	Oui	Non
Risque d'échec sur 0-day	Oui	Moins
Faux positifs	Peu	Beaucoup

3.2 Snort : L'Outil d'Analyse et de Prévention

Snort est un Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) open source qui exécute l'intégralité du cycle de détection :

1. **Capture :** Renifle les paquets réseau (comme un renifleur de paquets).
2. **Analyse :** Traite les paquets capturés.
3. **Recherche de Motif :** Compare le contenu et les métadonnées avec les règles définies.
4. **Alertes :** Déclenche une action (alerte, log, blocage).

3.2.1 Modes de Fonctionnement de Snort

Snort peut être configuré pour opérer dans trois modes principaux :

- **Renifleur de paquets** (Sniffer mode).
- **Logueur de paquets** (Logger mode).
- **IDS/IPS** (Network Intrusion Detection/Prevention System).

3.2.2 Composition et Syntaxe des Règles

Le mode IDS/IPS nécessite des **règles** (créées ou téléchargées) dont la structure est la suivante :

[Action] [Protocol] [IP source] [Port source] [Direction] [IP dest] [Port dest] [Options] (3.1)

Les composants clés sont :

- **Action :** Détermine la réaction de Snort (`alert`, `log`, `pass`, `drop`, `reject`, etc.).
- **Protocol :** Spécifie le protocole à surveiller (`TCP`, `UDP`, `ICMP`, `IP`).
- **Direction :** Indique le sens du trafic (`->` pour unidirectionnel, `<>` pour bidirectionnel).
- **Options :** Fournit des détails d'alerte ou de recherche de contenu (ex : `msg` pour le message, `sid` pour l'ID, `content` pour le contenu du paquet).

Exemples de Règles

Voici deux règles de signature de base :

Listing 3.1 – Règle d'alerte sur tout trafic ICMP (ping)

```
alert icmp any any -> any any (
  msg:"Traffic ICMP detecte";
  sid:1;
  metadata:policy security-ips alert;
  )
```

Listing 3.2 – Règle d'alerte sur toute tentative de connexion SSH

```
alert tcp any any -> any 22 (
  msg:"Tentative de connexion SSH";
  sid:2;
  metadata:policy security-ips alert;
)
```

3.2.3 Mise en Pratique : Configuration des Interfaces

Pour des tests concrets, Snort doit surveiller le trafic entre différents segments. La configuration typique sur une machine virtuelle de test implique au moins deux interfaces surveillées par Snort :

- **Interface 1 (Monitoring)** : `192.168.10.1/24` sur le segment LAN (Segment Interne).
- **Interface 2 (Monitoring)** : `192.168.20.1/24` sur le segment LAN (Segment Externe/DMZ).

Ceci permet de simuler un flux de trafic entre deux réseaux segmentés surveillé par l'IDS.