**Université Des Sciences et de la Technologie d’Oran Mohamed Boudiaf USTO-MB**

**Faculté des Mathématiques et Informatique**

**Département d’informatique**

**Sécurité Informatique 2024-2025**

 **Dr F.Khalifa**

**TD1 Principes de sécurité et techniques d’attaques**

**Exercice N°1 :**

La mise en place d’un vote électronique doit satisfaire aux 5 caractéristiques suivantes :

1. Seules les personnes autorisées à voter peuvent voter
2. Personnes ne peut voter plus qu’une fois,
3. Personnes ne peut déterminer pour qui quelqu’un d’autre a voté,
4. Personne ne peut modifier le vote de quelqu’un d’autre sans être découvert,
5. Tous les votants peuvent vérifier que leur vote a été pris en compte dans le décompte final,

Q1 Citer le service de sécurité correspondant a chacune de ces caractéristiques ?

Q2 Donnez pour chaque service de sécurité (citez dans Q1) l’attaque (les attaques) qui lui correspond? (répondre sous forme de tableau)

**Exercice N°2 :**

On considère un réseau local (LAN) composé de trois stations de travail et séparer de l’extérieur par un Serveur GW (passerelle). Les stations de travail sont configurées pour utiliser un serveur DNS 128.178.33.38 extérieur au LAN.



1. Réaliser une attaque de type ARP Spoofing , telle que l’intrus (station 2) va espionné une connexion **ftp** de provenance de la station 1 vers la station 3 et intercepter le mot de passe .

**Exercice 3**

Un intrus veut espionner une connexion **telnet** par une attaque vol de session TCP (hijaking), il forge un paquet TCP pour insérer la commande **\n écho HACKED \n** dans le flux de données. Le dernier échange de paquets avant l’insertion est illustrée dans la figure suivante.

Alice

Intrus

Bob

Alice.4335>bob.23 :200 (24) ack 700 "a"

bob.23>alice.4335 :700 (167) ack 224 "a"

Compléter cette figure par le paquet type TCP(hijaking) inséré par l’intrus et discuter les paquets qui suivent cette communication