

Exploiter les protocoles de communication

ESIR – SRIO

Djob Mvondo

Communication

- Vous avez établi un protocole de communication
- Comment un individu qui ne connaît pas le protocole peut vous empêcher de communiquer.... ?



Induire la victime en erreur

- Se placer en tant qu'un.e intermédiaire
- **Falsifier le message ou détruire son contenu**



Prérequis:

Induire la victime en erreur

- Se placer en tant qu'un.e intermédiaire
- **Falsifier le message ou détruire son contenu**



Prérequis:

1
Etre un
intermédiaire de
confiance

Induire la victime en erreur

- Se placer en tant qu'un.e intermédiaire
- **Falsifier le message ou détruire son contenu**



Prérequis:

1
Etre un
intermédiaire de
confiance

2
Pouvoir
intercepter le
message

Induire la victime en erreur

- Se placer en tant qu'un.e intermédiaire
- **Falsifier le message ou détruire son contenu**



Prérequis:

1
Etre un
intermédiaire de
confiance

2
Pouvoir
intercepter le
message

3
Ne pas modifier
le flux applicatif
normal

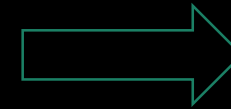
MITM: Man In The Middle Attack

- Se déroule en deux phases
 - **Interception** : Intercepter la communication avant son arrivée à destination
 - **Décodage** : Décoder l'information pour soit altérer son contenu, ou récupérer des données sensible pour exploiter plus tard.

MITM: Man In The Middle Attack

- Se déroule en deux phases

- **Interception** : Intercepter la communication avant son arrivée à destination
- **Décodage** : Décoder l'information pour soit altérer son contenu, ou récupérer des données sensible pour exploiter plus tard.



- ☐ Sur un **réseau public**
- ☐ Dans un **réseau privé où vous et le malfaiteur avez accès**
- ☐ Vous induire dans un **réseau malsain**.

MITM: Man In The Middle Attack

- Se déroule en deux phases

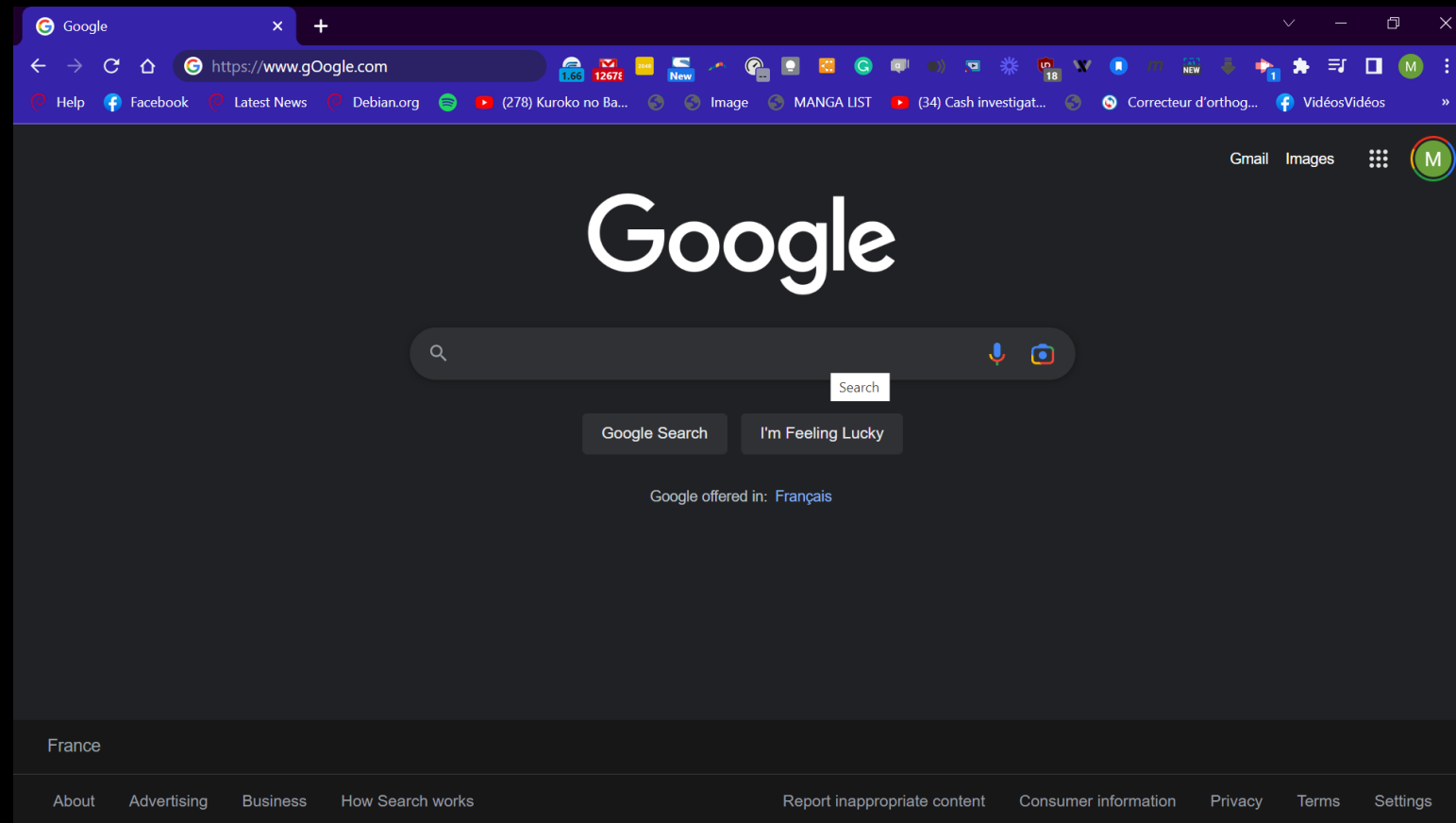
- **Interception** : Intercepter la communication avant son arrivée à destination
- **Décodage** : Décoder l'information pour soit altérer son contenu, ou récupérer des données sensible pour exploiter plus tard.



- ☐ Sur un **réseau public**
- ☐ Dans un **réseau privé où vous et le malfaiteur avez accès**
- ☐ Vous induire dans un **réseau malsain**.
- ☐ Vous forcer à **entrer des données** ou à **réaliser une action précise**
- ☐ Se faire **passer pour vous** pour avoir plus de droits.

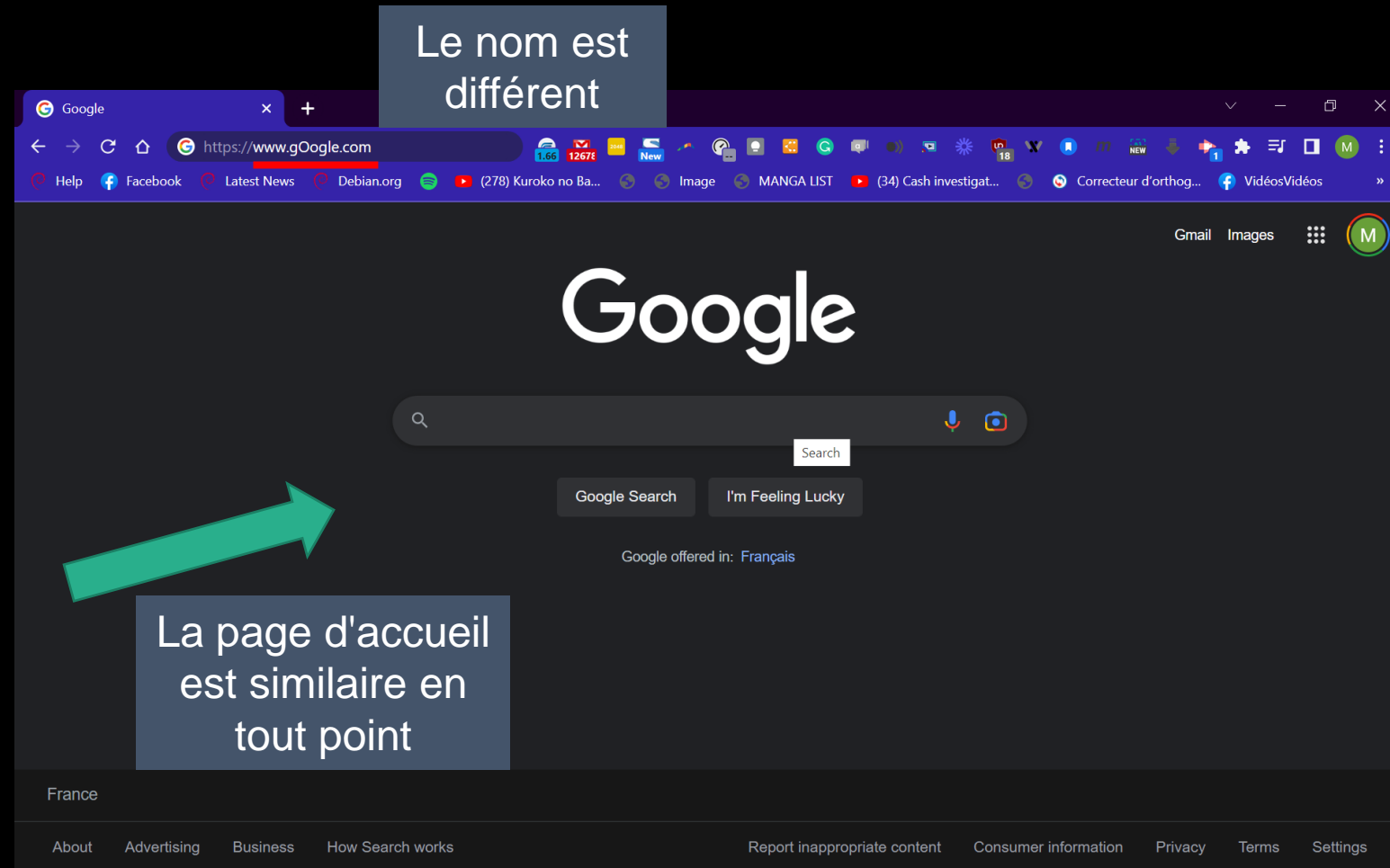
MITM: Man In The Middle Attack

Un cas pratique : Que remarquez-vous ?



MITM: Man In The Middle Attack

Un cas pratique : Que remarquez-vous ?



MITM: Man In The Middle Attack

Un cas pratique : Que remarquez-vous ?

The image shows a screenshot of the Google homepage with several annotations in French. A grey box at the top center contains the text "Le nom est différent" (The name is different), with a white arrow pointing to the right towards the text "Un routeur + Résolution de DNS local + payer un certificat (automatique avec un routeur)". A green arrow points from the bottom left towards the search bar area, with a grey box below it containing the text "La page d'accueil est similaire en tout point" (The homepage is similar in every point). A white arrow points from this box to the text "HTML+CSS". The screenshot itself shows the Google logo, search bar, and navigation links at the bottom.

Le nom est différent

Un routeur + Résolution de DNS local + payer un certificat (automatique avec un routeur)

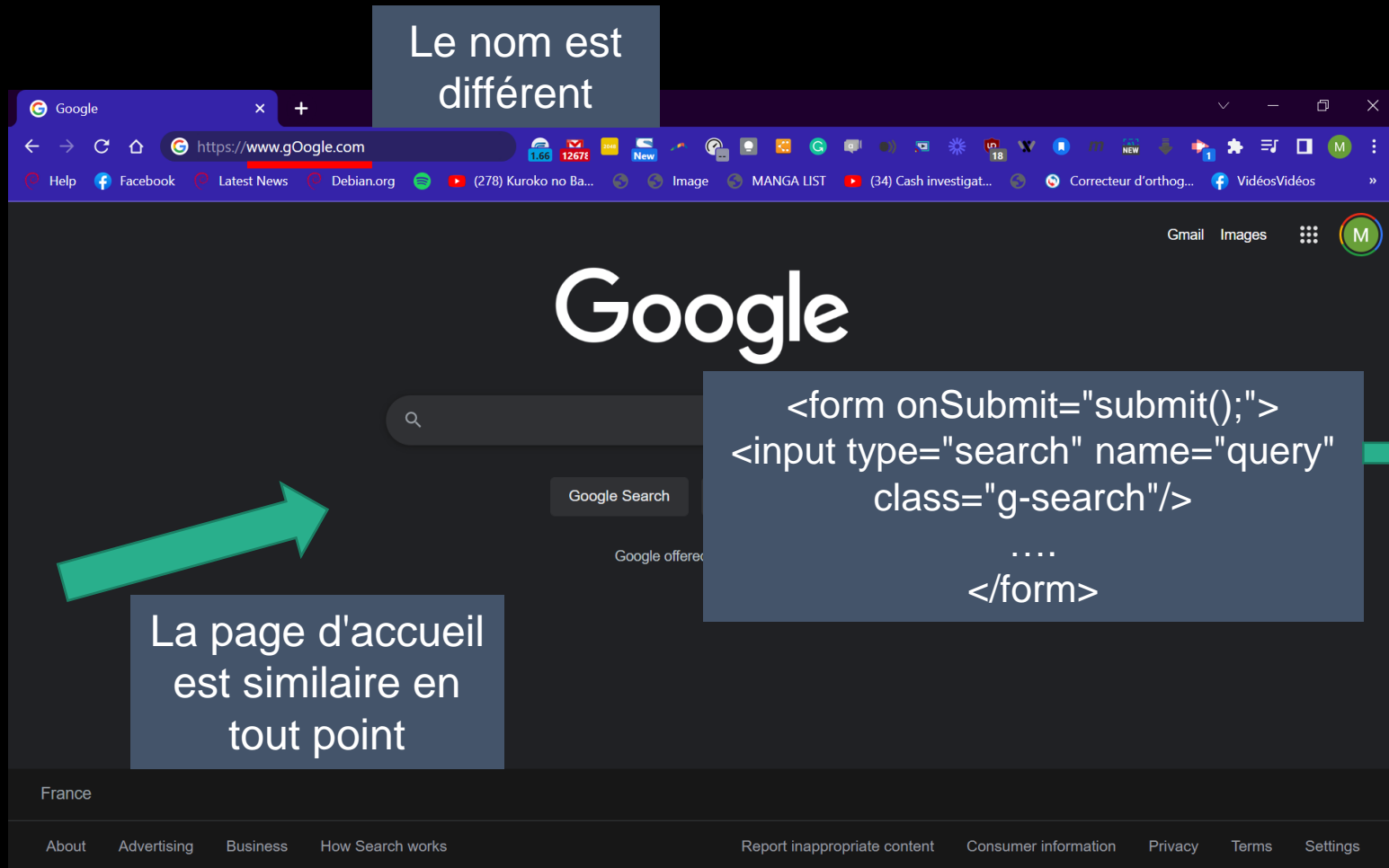
La page d'accueil est similaire en tout point

HTML+CSS

MITM: Man In The Middle Attack

Un cas pratique : Que remarquez-vous ?

Le nom est différent



The screenshot shows the Google homepage in a web browser. A green arrow points from the search bar area to a text box containing HTML code. Another green arrow points from the same text box to a code editor on the right. A third green arrow points from the bottom left of the page to a text box.

La page d'accueil est similaire en tout point

```
<form onSubmit="submit();">
<input type="search" name="query"
class="g-search"/>
....
</form>
```

Que fais ce code ?



```
const express = require('express')
const app = express()

app.use(express.urlencoded({
  extended: true
}))

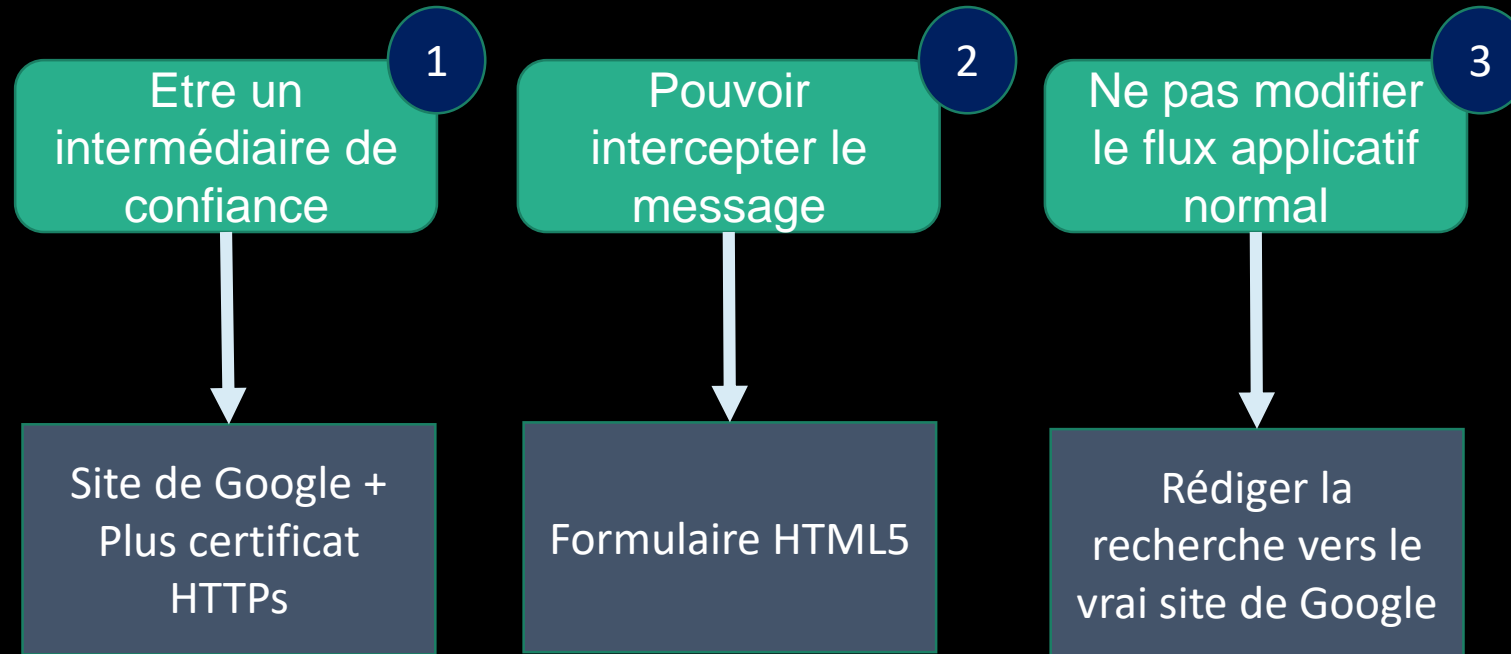
app.post('/submit-form', (req, res) => {
  const query = req.body.query
  //save it locally or database
  ...
  res.writeHead(302, {
    location:
      "https://google.com/search"+
        "?q="+query,
  });
  res.end()
})
```

MITM: Man In The Middle Attack

Un cas pratique : Que remarquez-vous ?

Que fais ce code ?

Prérequis:



MITM: Man In The Middle Attack

Plusieurs variantes existent mais repose sur les mêmes mécanismes.

Injection de
paquets

Vol de session

Inspection de
paquets

Communication

- Vous avez établi un protocole de communication
- Comment un individu qui ne connaît pas le protocole peut vous empêcher de communiquer.... ? → La surcharge



Vous surcharger d'informations

- Qu'arrive t'il lorsqu'on est surchargé ?

Ca devient très compliqué de continuer

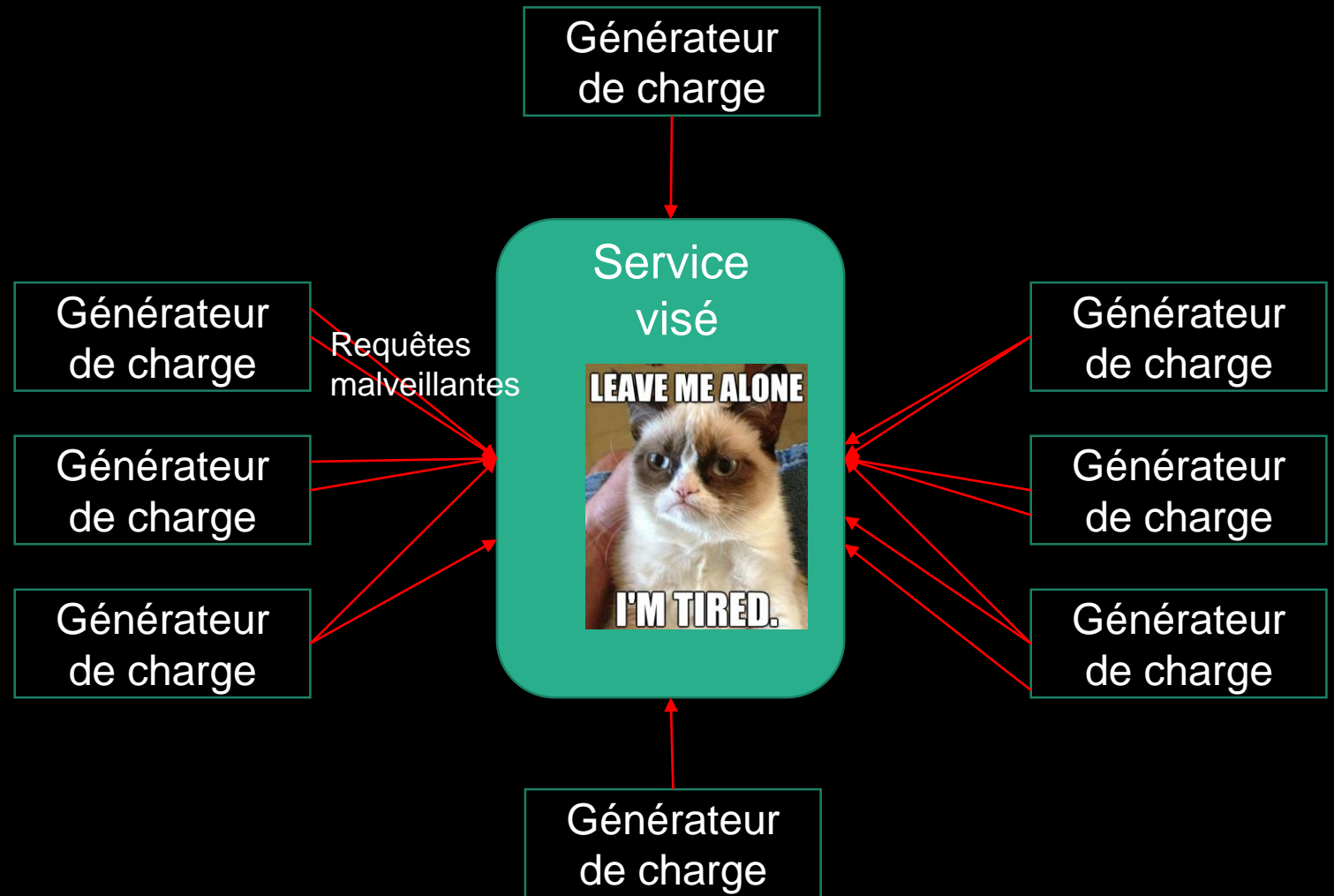
Même principe pour un équipement dans un réseau :
S'il est surchargé, il ne fonctionnera plus correctement



(D)DOS : (Distributed) Denial of Service

L'objectif d'une telle attaque est d'empêcher un système de fonctionner dû à une surcharge de requêtes. Les causes d'une telle attaque sont compliqué à réparer et porte énormément préjudice.

- ❖ Le système visé ne peut donc plus assurer le service qu'il doit
- ❖ Le système visé devient corrompu dû à des erreurs d'exécution
- ❖ Le système visé ne peut être restauré



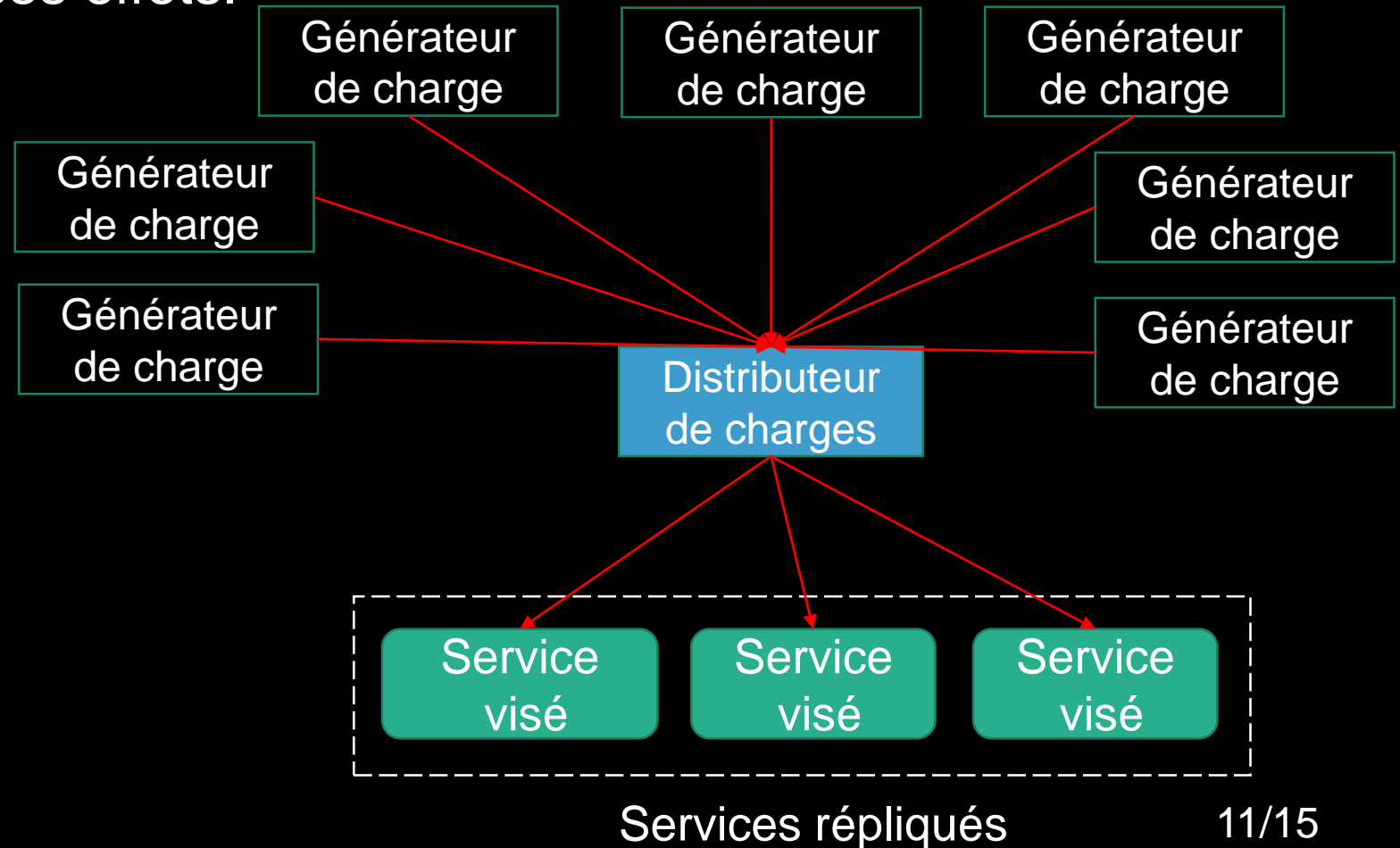
(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Répliquer ses services sur plusieurs équipements

Un distributeur de charges répartir les requêtes entre les différents équipements.

Théorie algorithmique sur le nombre de répliques à maintenir



(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Réutiliser au maximum
les connexions



Exploiter les **pool** dans
vos programmes pour
optimiser l'utilisateur
des ressources

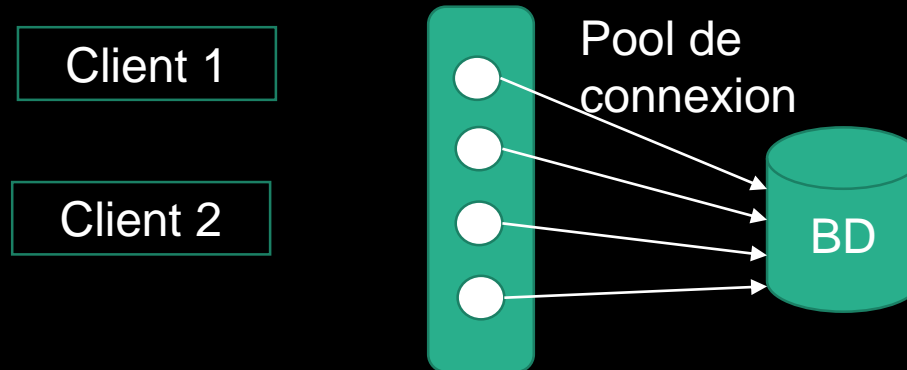
Ne pas créer une nouvelle
connexion ou socket pour
chaque requête

(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Réutiliser au maximum
les connexions

Ne pas créer une
nouvelle connexion ou
socket pour chaque
requête



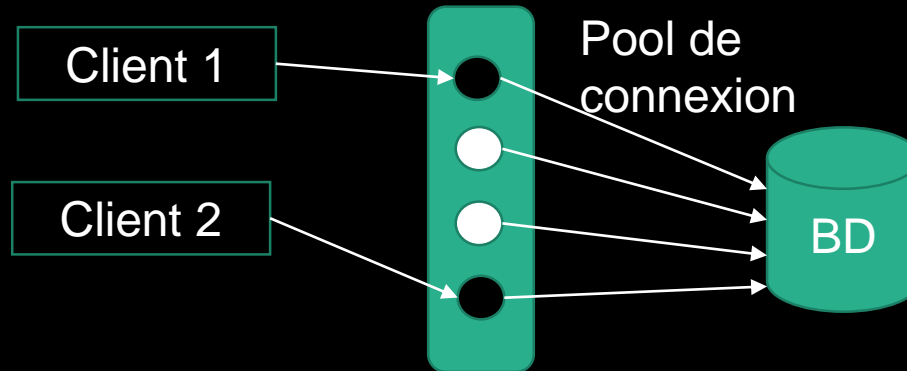
Supposons un pool de 4 connexions.

(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Réutiliser au maximum
les connexions

Ne pas créer une
nouvelle connexion ou
socket pour chaque
requête



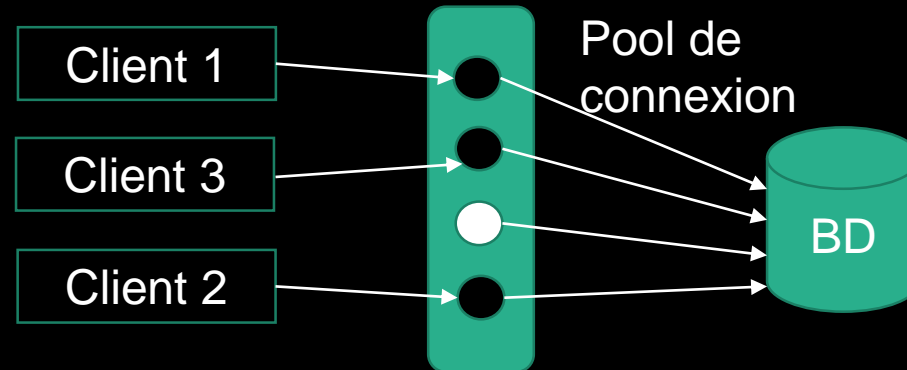
Deux clients envoient des requêtes.
Deux instances du pool sont réquisitionnées.

(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Réutiliser au maximum
les connexions

Ne pas créer une
nouvelle connexion ou
socket pour chaque
requête



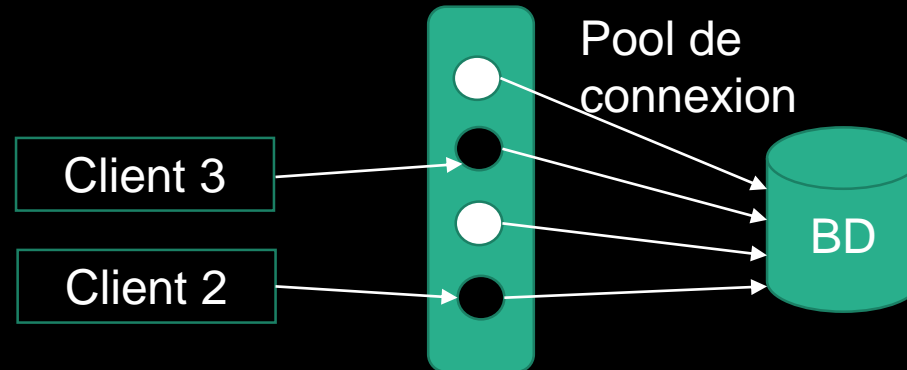
Un troisième client envoie une requête.
Une instance libre lui est attribuée.

(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Réutiliser au maximum
les connexions

Ne pas créer une
nouvelle connexion ou
socket pour chaque
requête



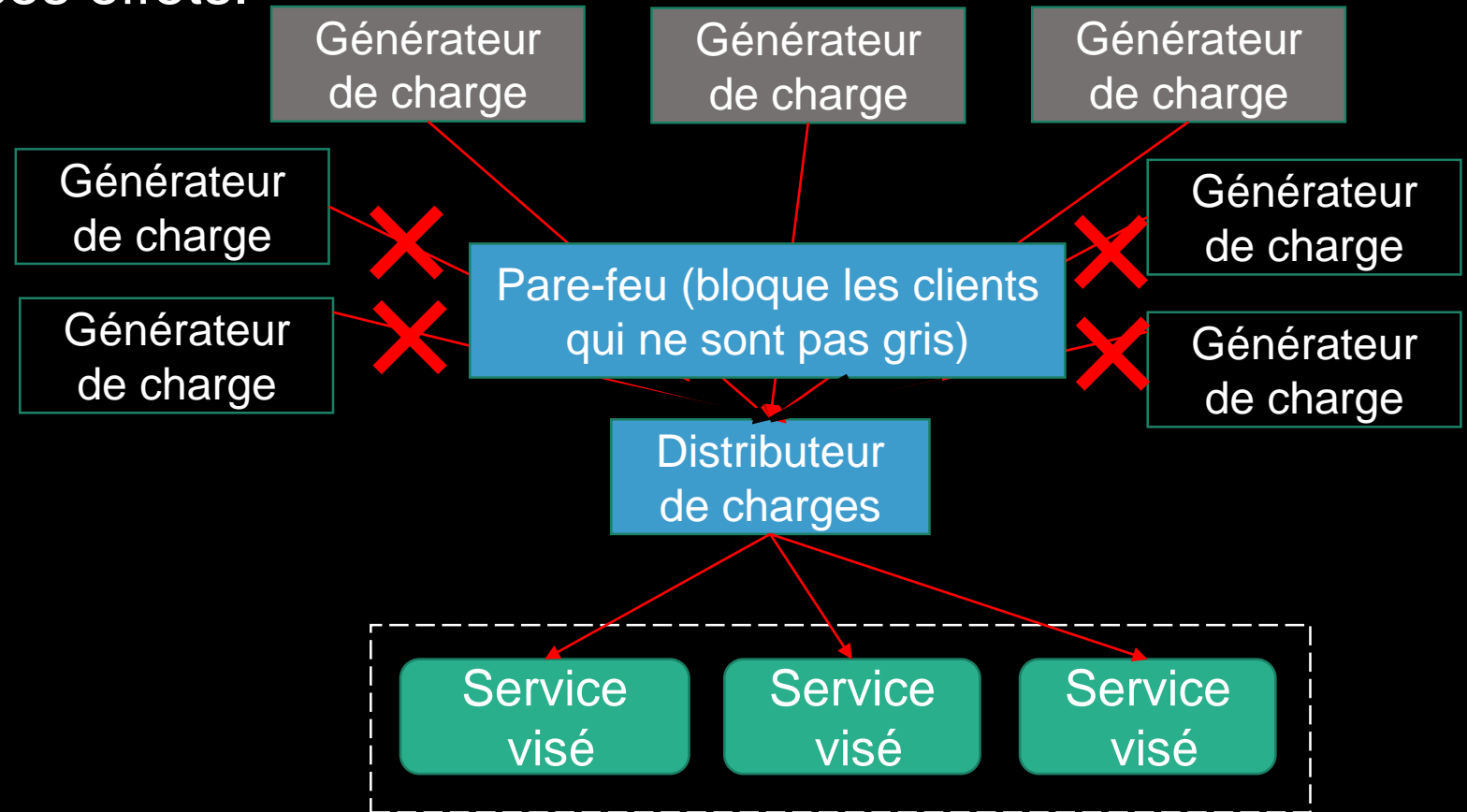
Le client 1 termine et relâche l'instance pour
une autre client. Ainsi de suite sans créer
une nouvelle connexion à chaque fois.

(D)DOS : (Distributed) Denial of Service

Elle est restée une attaque facile à mettre sur pied surtout si on a la puissance de calcul associée. Néanmoins, plusieurs techniques peuvent être utilisées pour limiter ses effets.

Filtrer les clients avec des pare-feus ou ACLs (Access Control List)

Réduit le nombre de personnes qui peuvent envoyer une requête si vous avez une clientèle spécifique



Devoir 4

Documentez vous sur les différentes variantes des MITM et DDOS.

Faîtes un résumé (pas de limite de mots) des différentes variantes que vous avez compris en essayant d'illustrer au maximum et en ressortissant les mécanismes utilisés.