Présentation

Attaques en contexte « Man-in-the-Middle »

Par Martin Dubé
2011-09-27

Avertissement

Ce qui suit est présenté à titre éducatif...

Table des matières

Qu'est-ce qu'une attaque de type « Man-in-the-Middle »?

- Attaque menée par un individu dont l'intention est d'intercepter, rediriger, lire ou modifer le trafic échangé entre les victimes de son choix

- Limites
  - Nécessite une connexion physique (une « patte ») sur un réseau local ciblé
    - → Une prise de contrôle à distance illicite peut très bien convenir
      - « Backdoor »
      - « Reverse Shell »
      - Etc.
  - Le choix des victimes est limité au segment réseau de l'attaquant

Environnement de la présentation

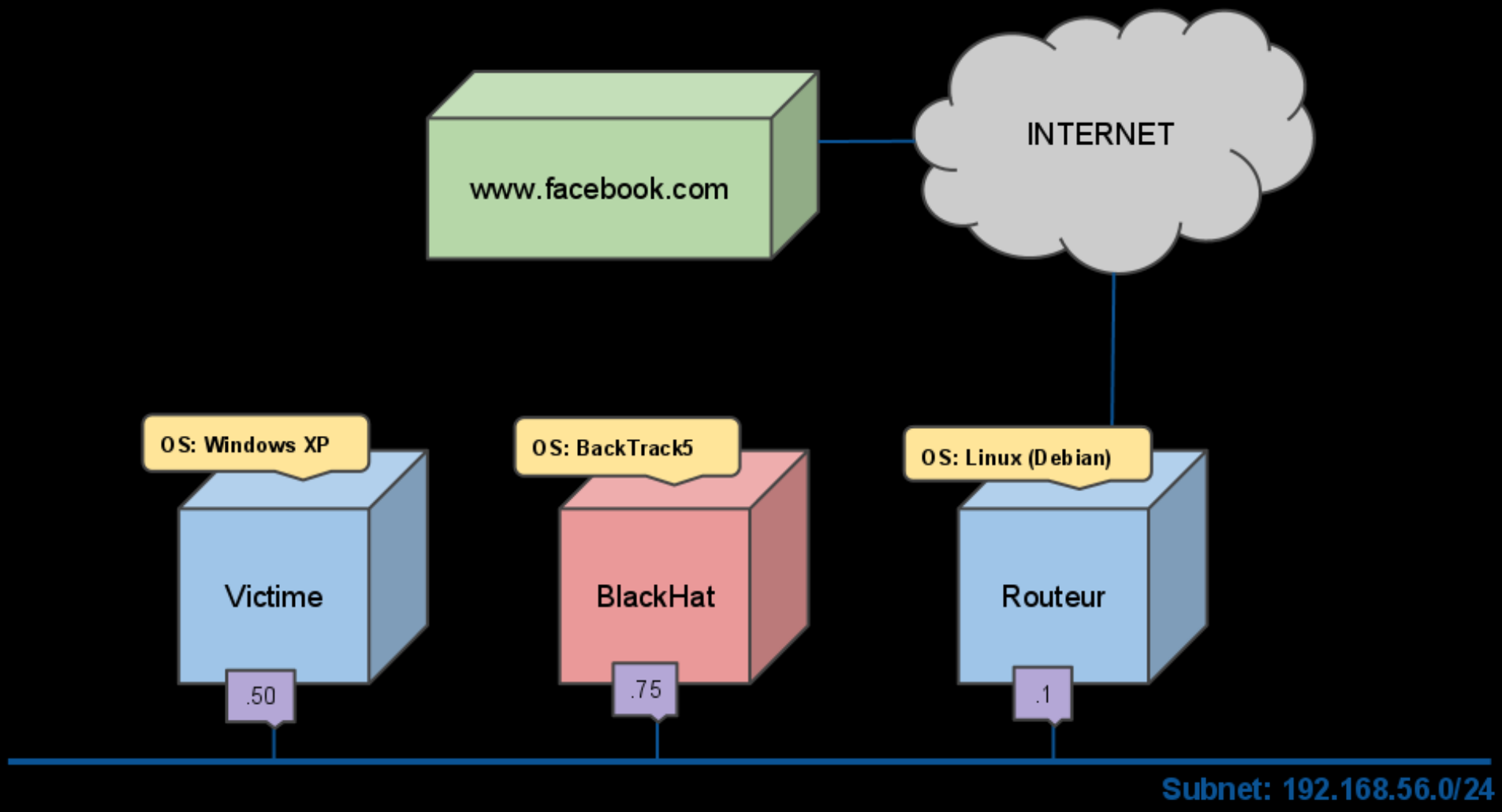


Table des matières

Quelques notions de réseau

- Couches OSI
  - 7. Application
    - NNTP · SIP · SSI · DNS · FTP · Gopher · HTTP · NFS · NTP · SMPP · SMTP · SNMP · Telnet · DHCP · Netconf · RTP ·
  - 6. Présentation
    - MIME · XDR · TLS · SSL
  - 5. Session
    - Named Pipes · NetBIOS · SAP · L2TP · PPTP · SPDY
  - 4. Transport
    - TCP · UDP · SCTP · DCCP · SPX
  - 3. Réseau
    - IP (IPv4, IPv6) · ICMP · IPsec · IGMP · IPX · AppleTalk
  - 2. Liaison de données
    - ATM · SDLC · HDLC · ARP · CSLIP · SLIP · GFP · PLIP · IEEE 802.3 · Frame Relay · ITU-T G.hn DLL · PPP · X.25 · Network Switch ·
  - 1. Physique
    - EIA/TIA-232 · EIA/TIA-449 · ITU-T V-Series · I.430 · I.431 · POTS · PDH · SONET/SDH · PON · OTN · DSL · IEEE 802.3 · IEEE 802.11 · IEEE 802.15 · IEEE 802.16 · IEEE 1394 · ITU-T G.hn PHY · USB · Bluetooth · Hubs

Quelques notions de réseau

- Une adresse IP (Internet Protocol) identifie un hôte dans un inter-réseau (ex : internet)
- Par contre, dans un segment réseau (local), un hôte est identifié par son adresse MAC
- De plus, cette même adresse MAC contraint un hôte à n'envoyer des paquets qu'à l'intérieur de son propre segment réseau
- Que se passe-t-il si la destination est sur un segment différent (ex. internet)???
- Comment déterminer l'adresse MAC?

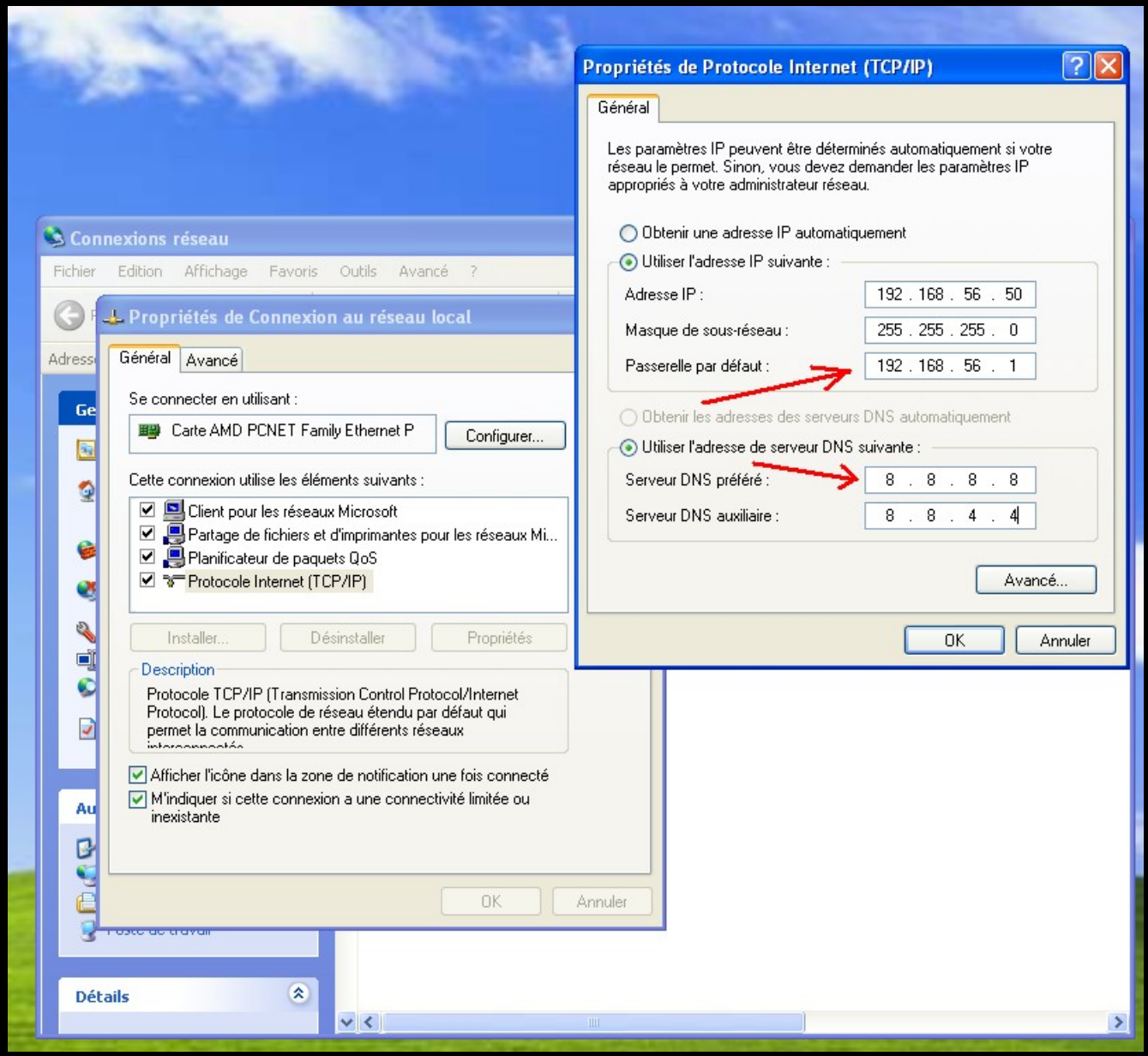
Quelques notions de réseau

- La passerelle par défaut est utilisé pour acheminer les paquets vers l'extérieur
- Le protocole ARP résoud l'adresse IP en adresse MAC

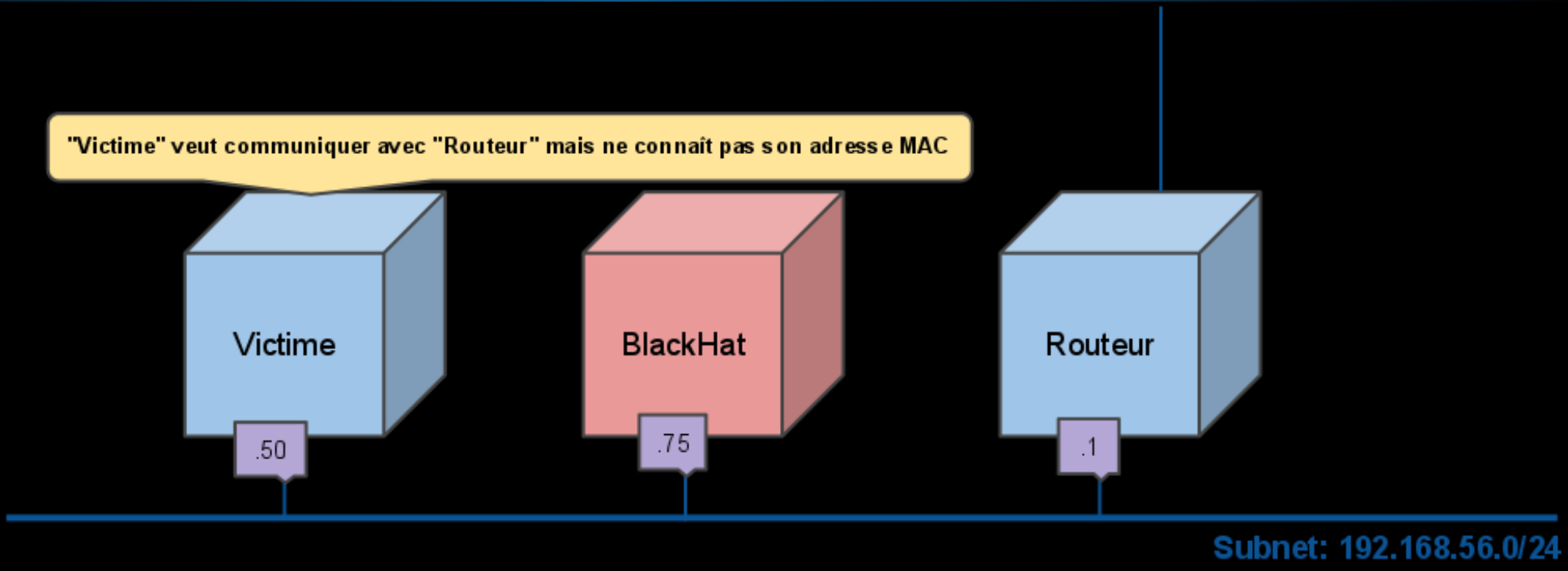
Quelques notions de réseau

- Exemple : Un poste veut accéder à www.facebook.com
  - 1- Ouverture du navigateur + Taper « www.facebook.com »
  - 2- Le navigateur interroge un serveur DNS
    - Résolution du nom « www.facebook.com »
    - Obtention de l'adresse IP : 69.171.228.13
  - 3- Il est calculé si l'adresse est externe ou interne
    - 192.168.56.50 & 255.255.255.0 = 192.168.56.0
    - Est-ce que 69.171.228.13 fait parti de 192.168.56.0? non!
  - 4- Dans le cas présent, l'adresse est externe
    - Les paquets devront donc transiter par la passerelle par défaut du segment
  - 5- Résolution ARP sur l'adresse IP de la passerelle
    - Transformer 192.168.56.1 par 22:22:22:22:22:22
  - 6- L'adresse IP & MAC destination étant connu, le paquet peut être acheminé et la requête complétée bout-en-bout
    - Résultat : Affichage de la page de facebook
  - Note : Processus complètement transparent pour un utilisateur

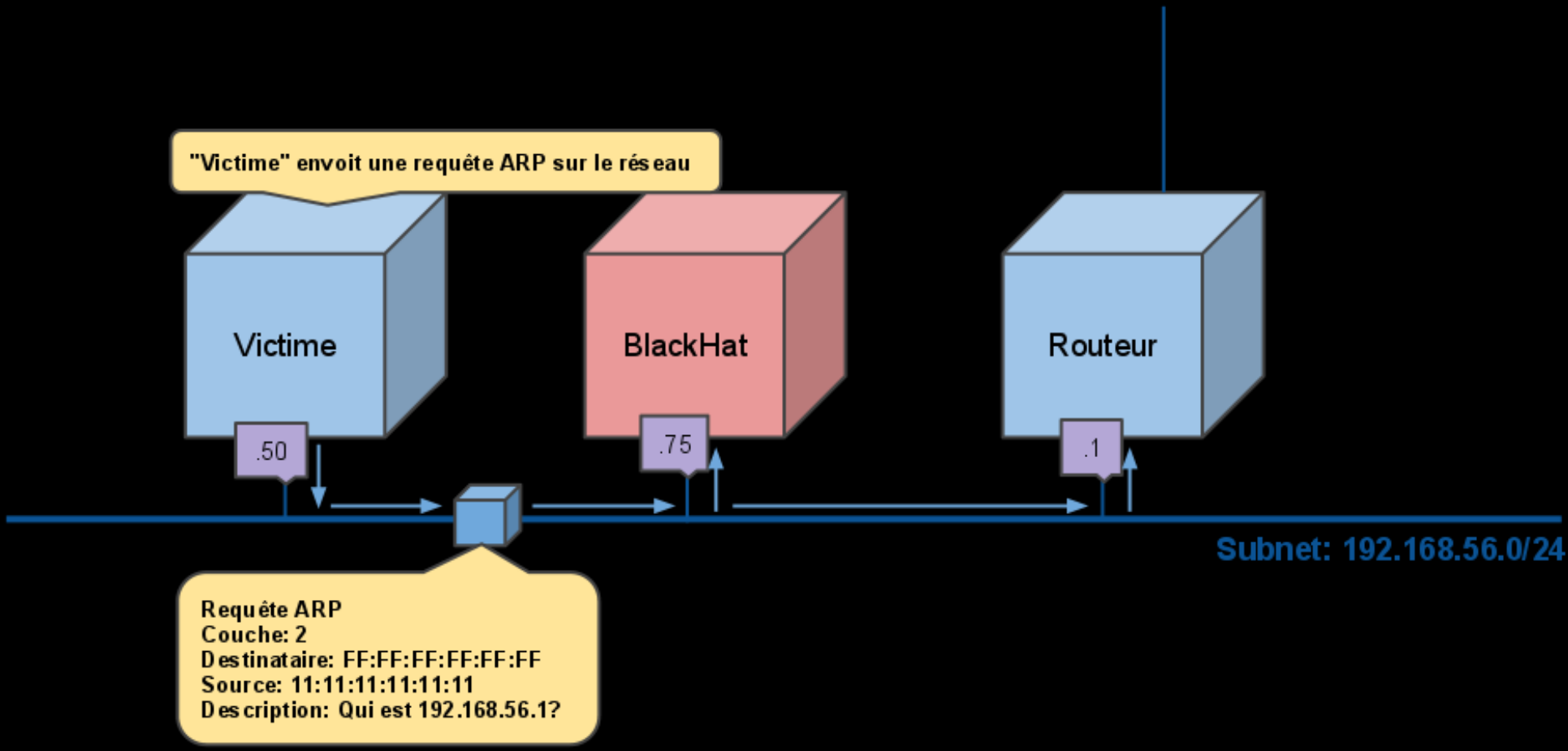
Quelques notions de réseau



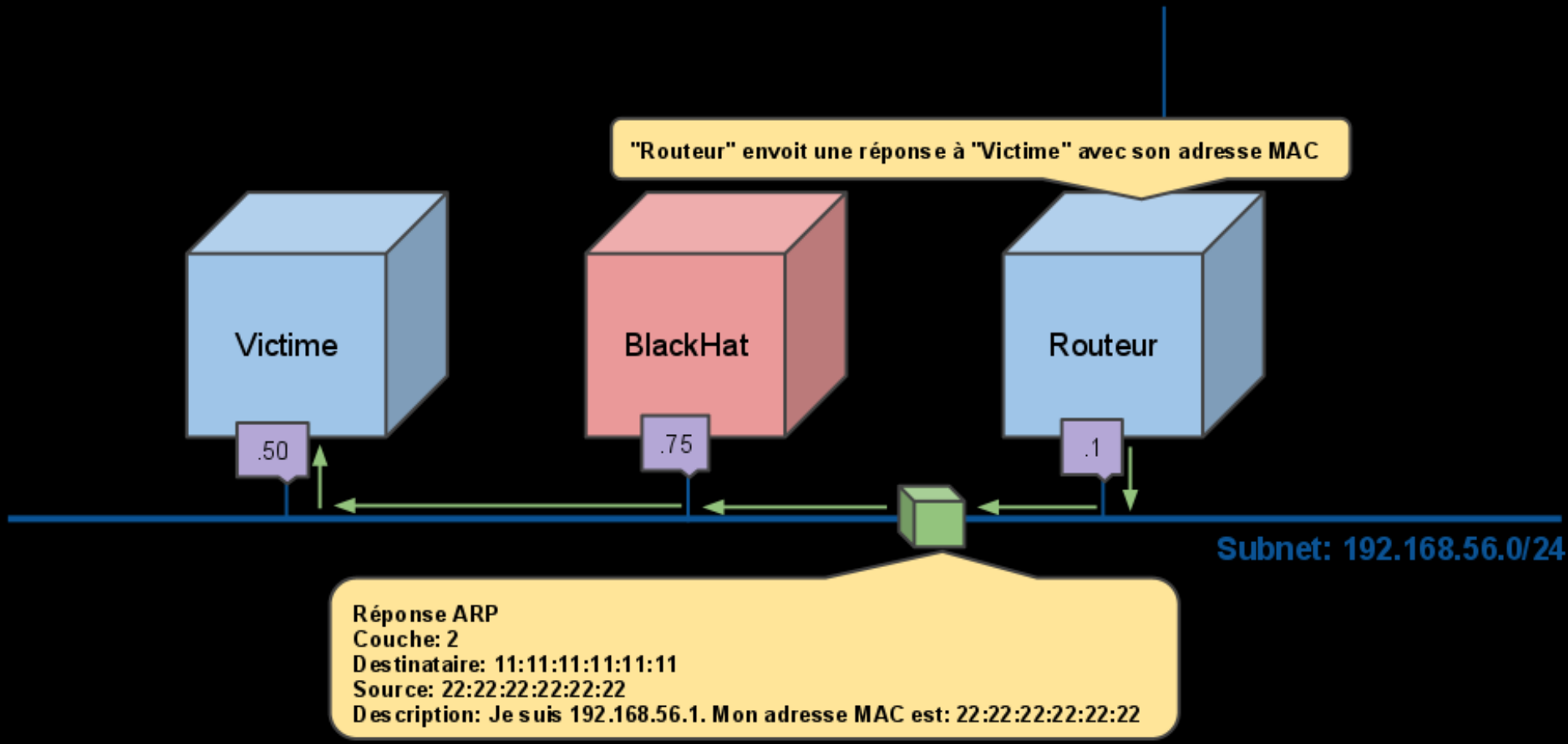
Explications du protocole ARP



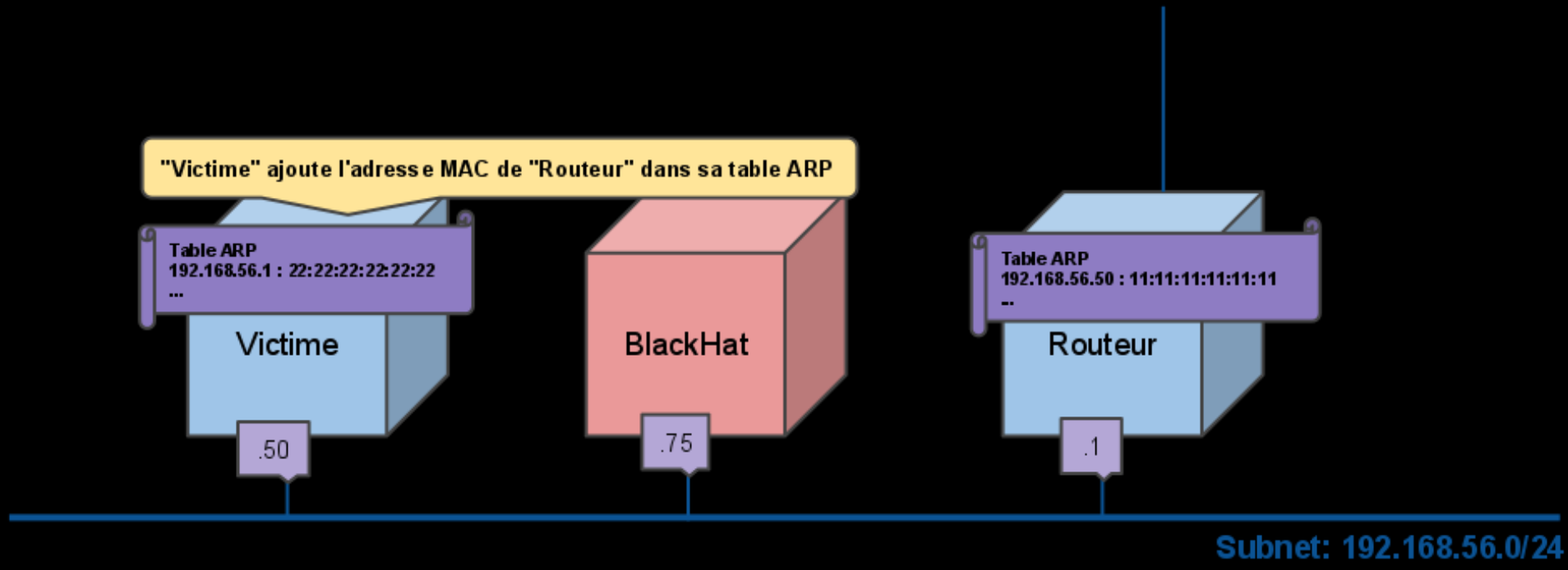
Explications du protocole ARP



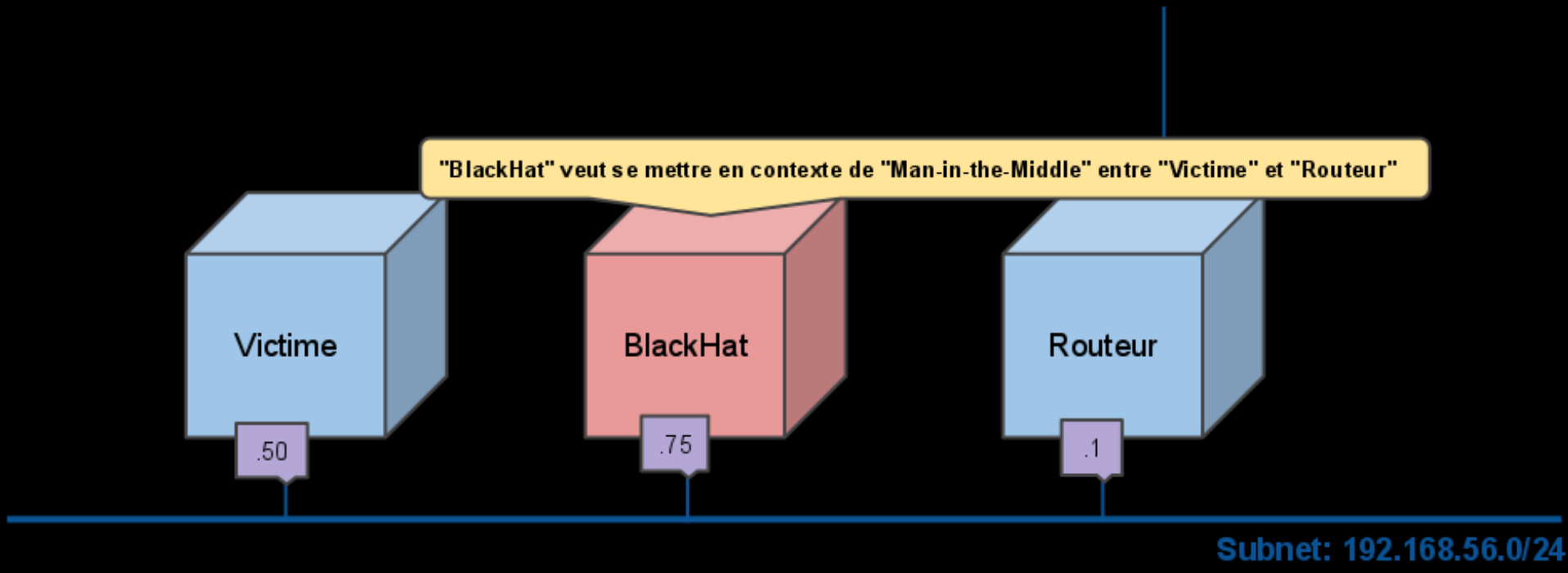
Explications du protocole ARP



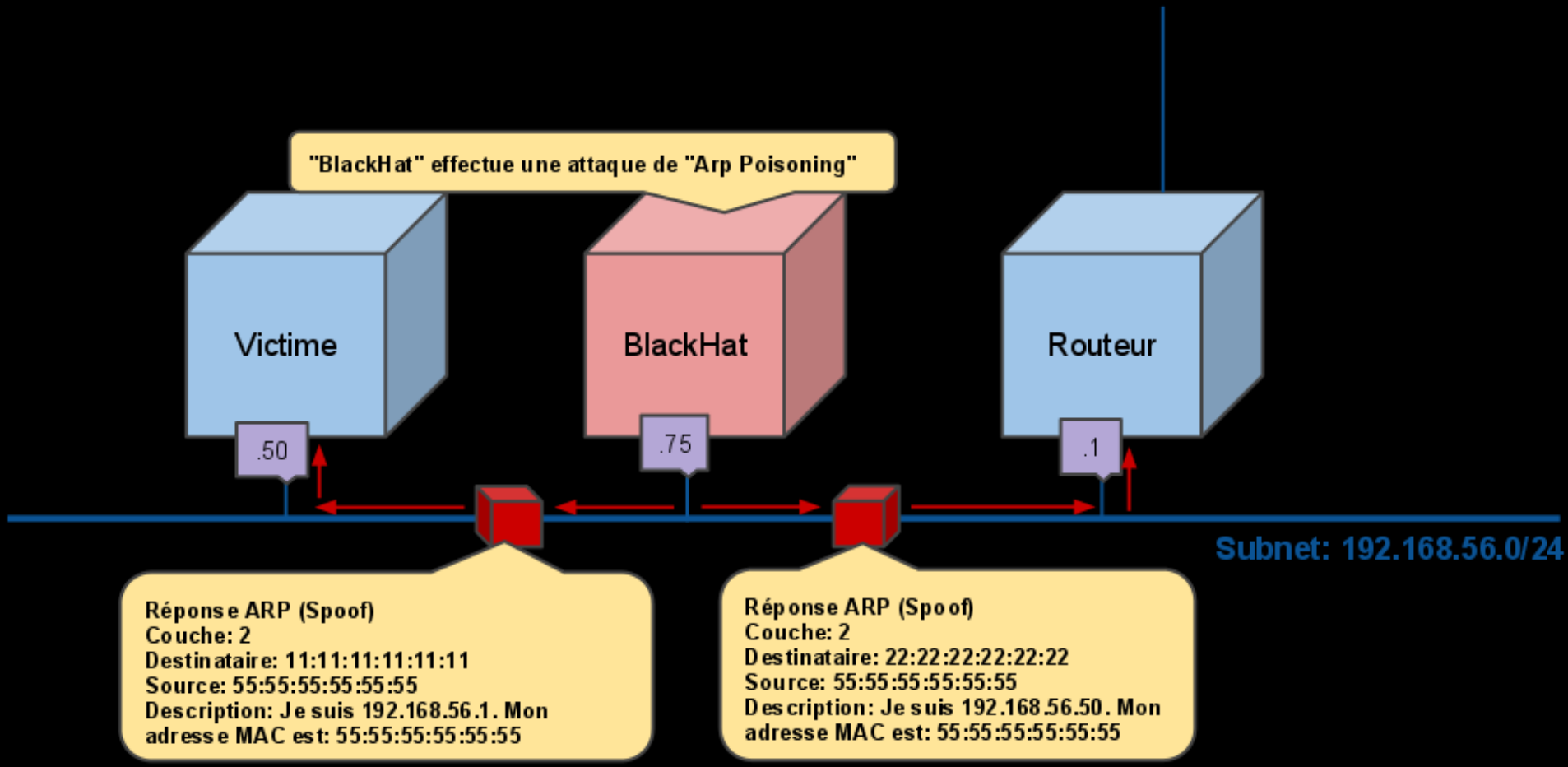
Explications du protocole ARP



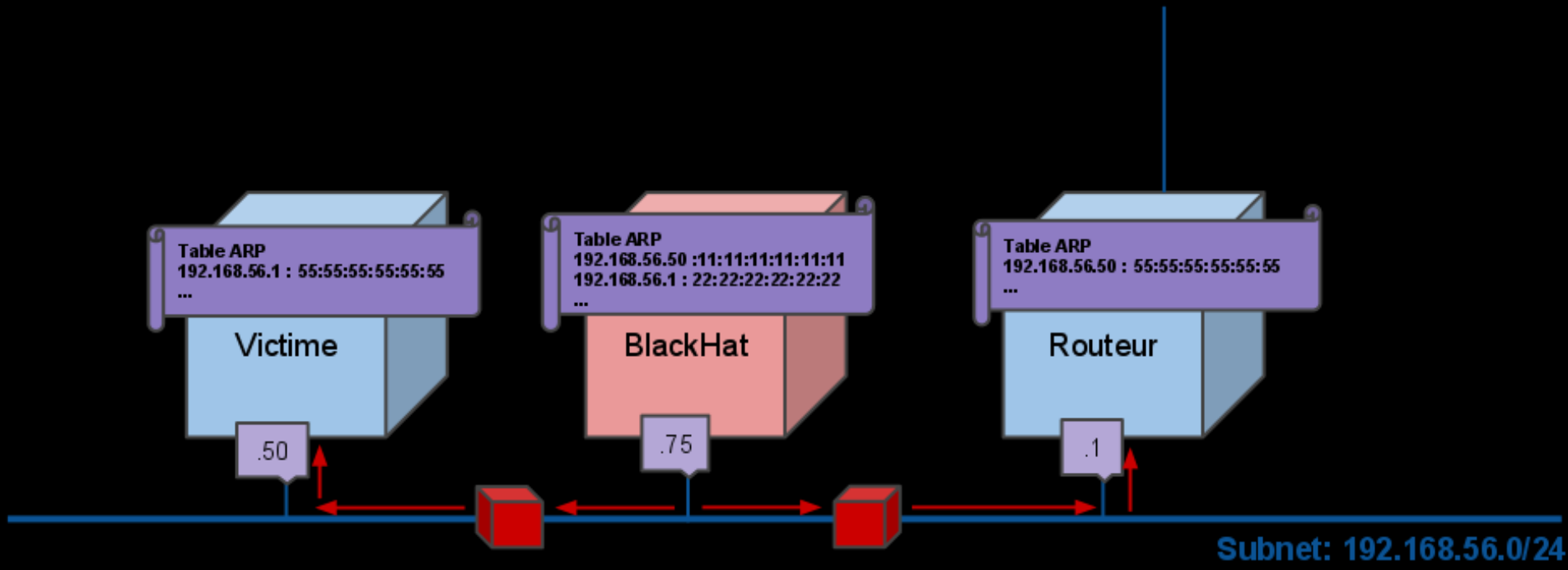
Explications du « Arp Poisoning »



Explications du « Arp Poisoning »



Explications du « Arp Poisoning »

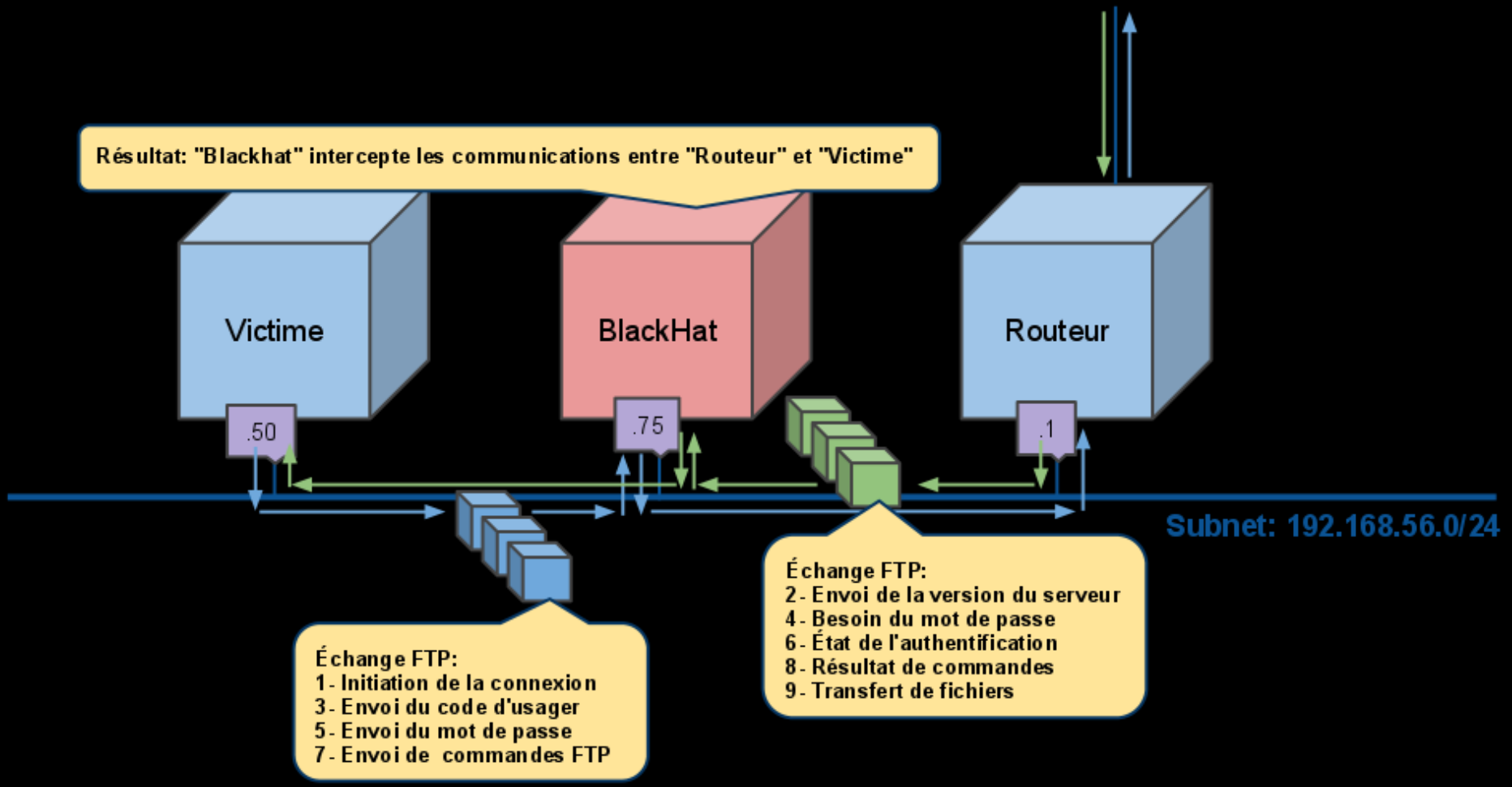


Démo

Mise en contexte
« Arp Poisoning »

Table des matières

« Sniffing »


Résultat: "Blackhat" intercepte les communications entre "Routeur" et "Victime"
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Échange FTP:
1- Initiation de la connexion
3- Envoi du code d'usager
5- Envoi du mot de passe
7- Envoi de commandes FTP
Échange FTP:
2- Envoi de la version du serveur
4- Besoin du mot de passe
6- État de l'authentification
8- Résultat de commandes
9- Transfert de fichiers

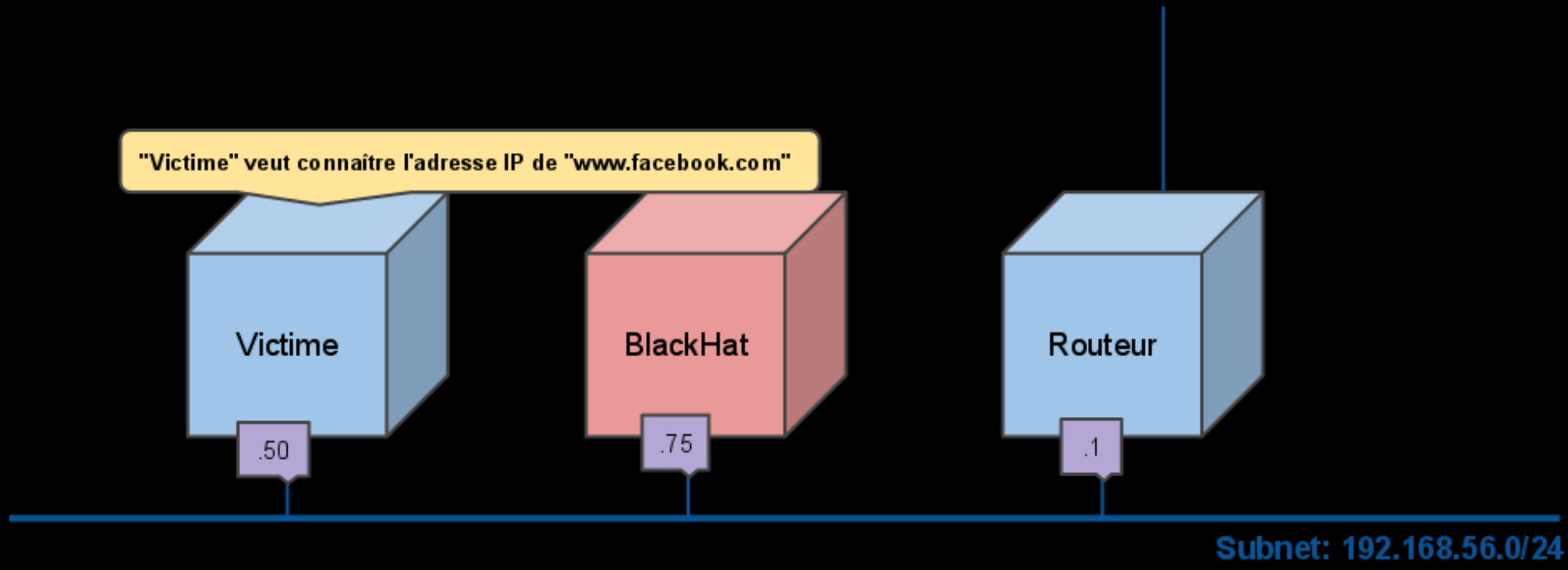
Démo

Attaque #1

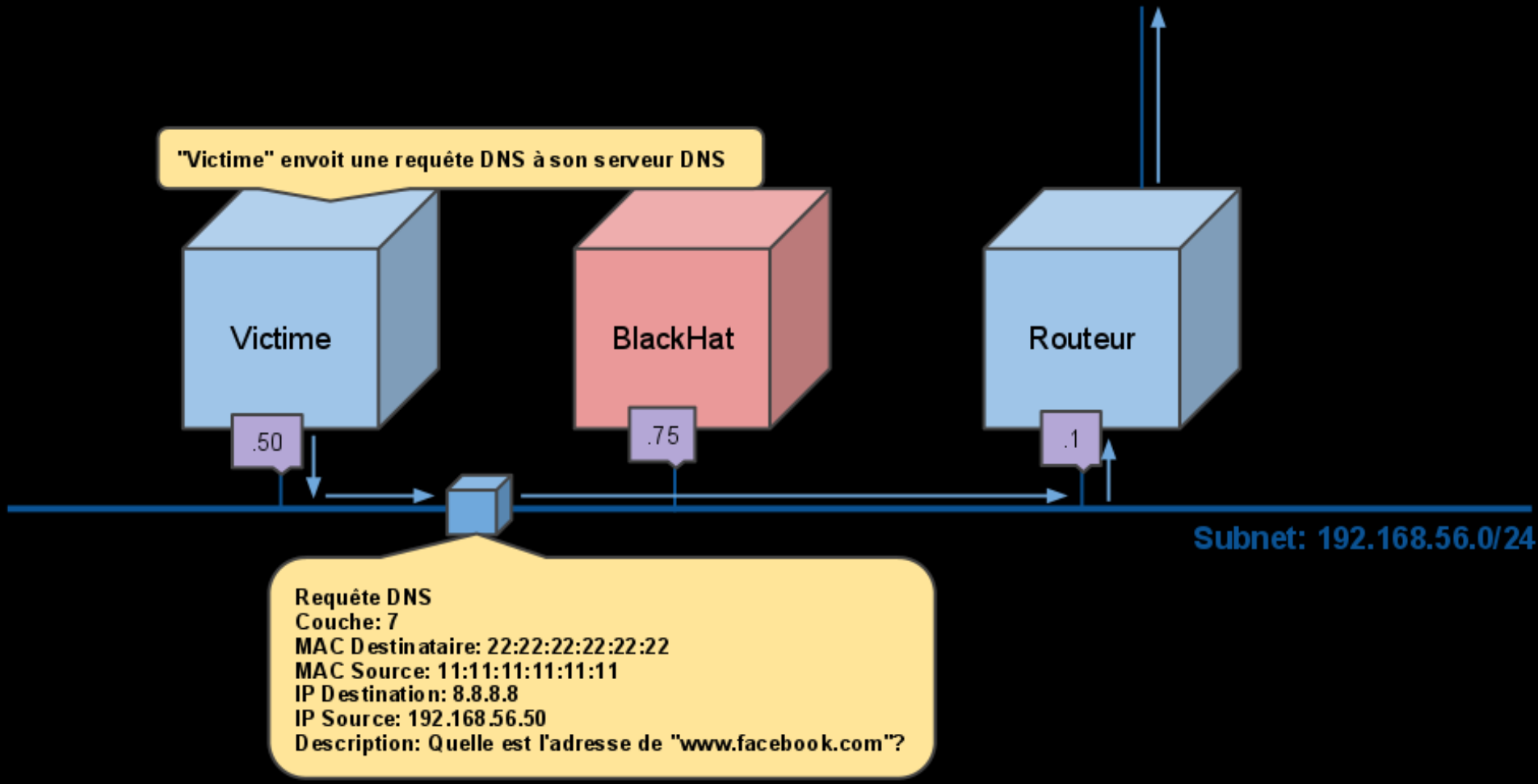
« Sniffing »

Table des matières

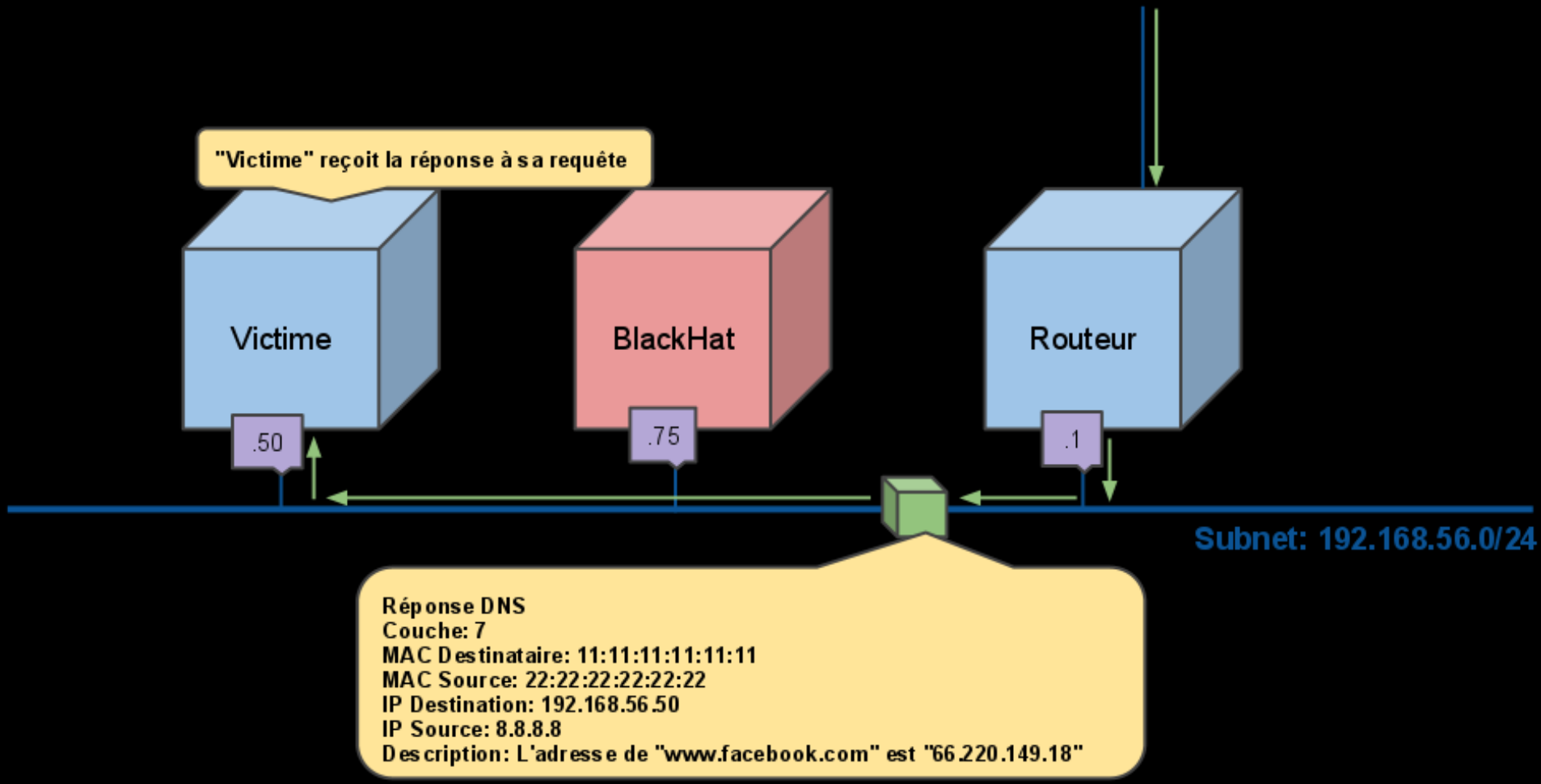
Protocole DNS



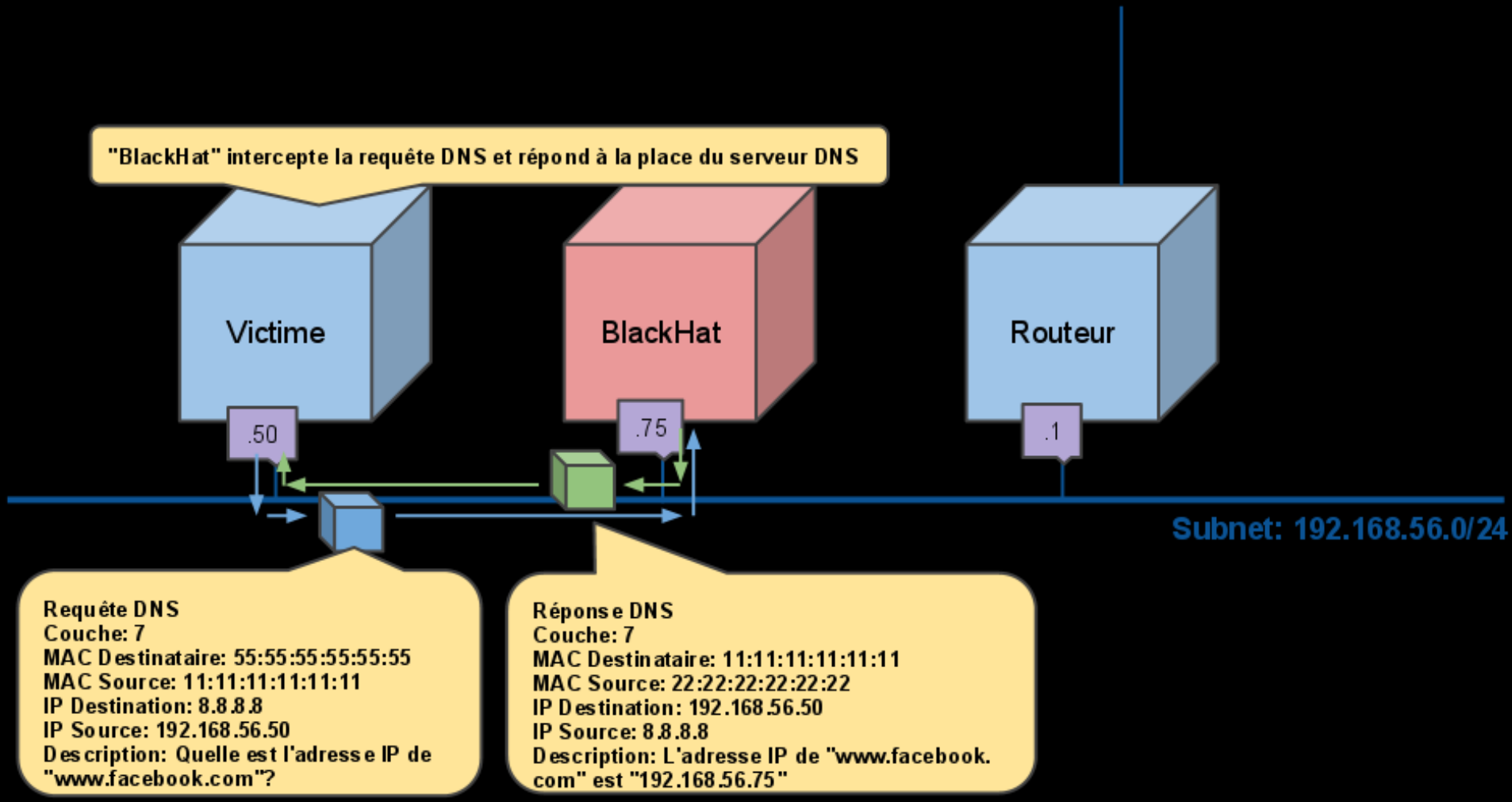
Protocole DNS



Protocole DNS



Explications d'un « DNS Redirection »



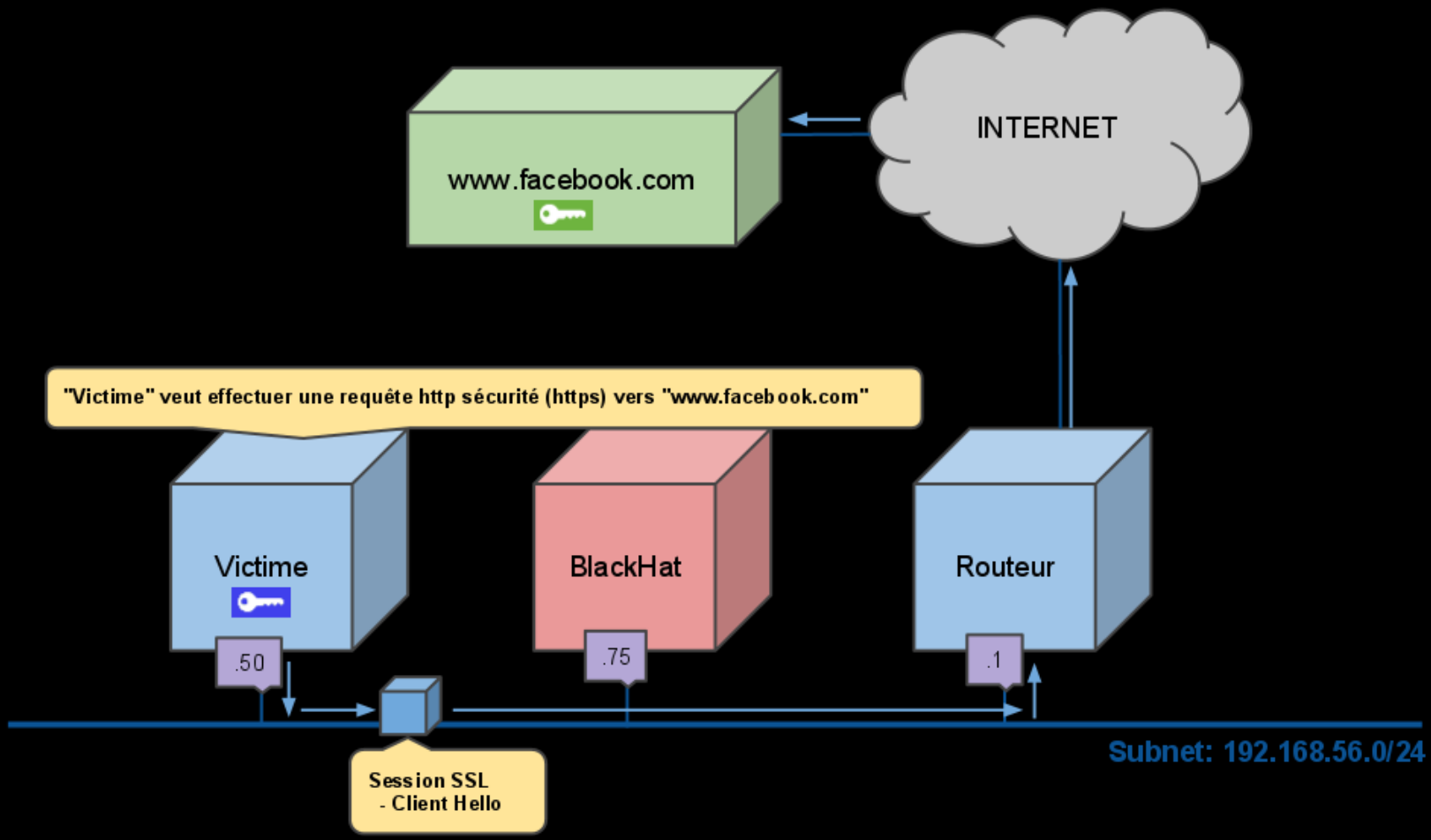
Démo

Attaque #2

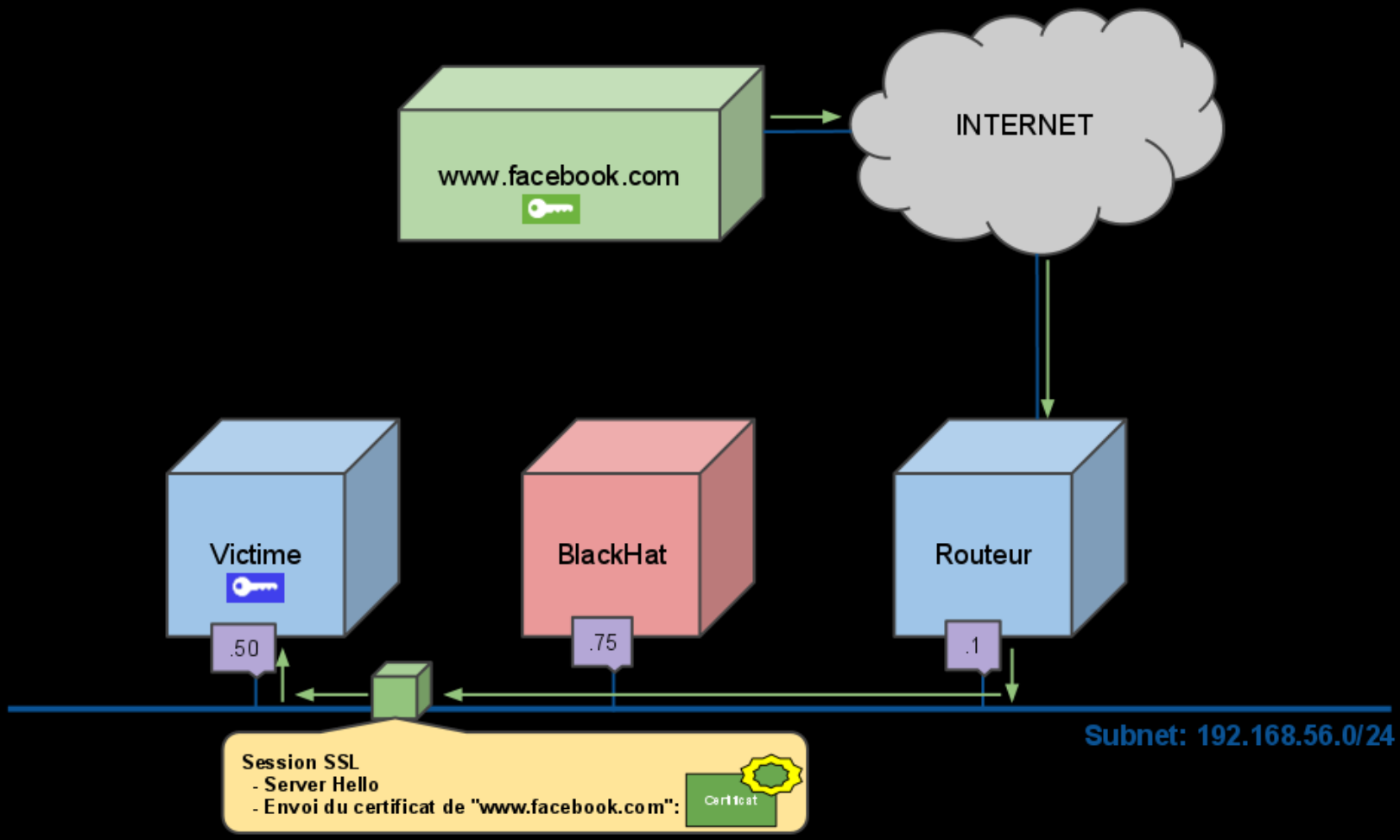
« DNS Redirection »

Table des matières

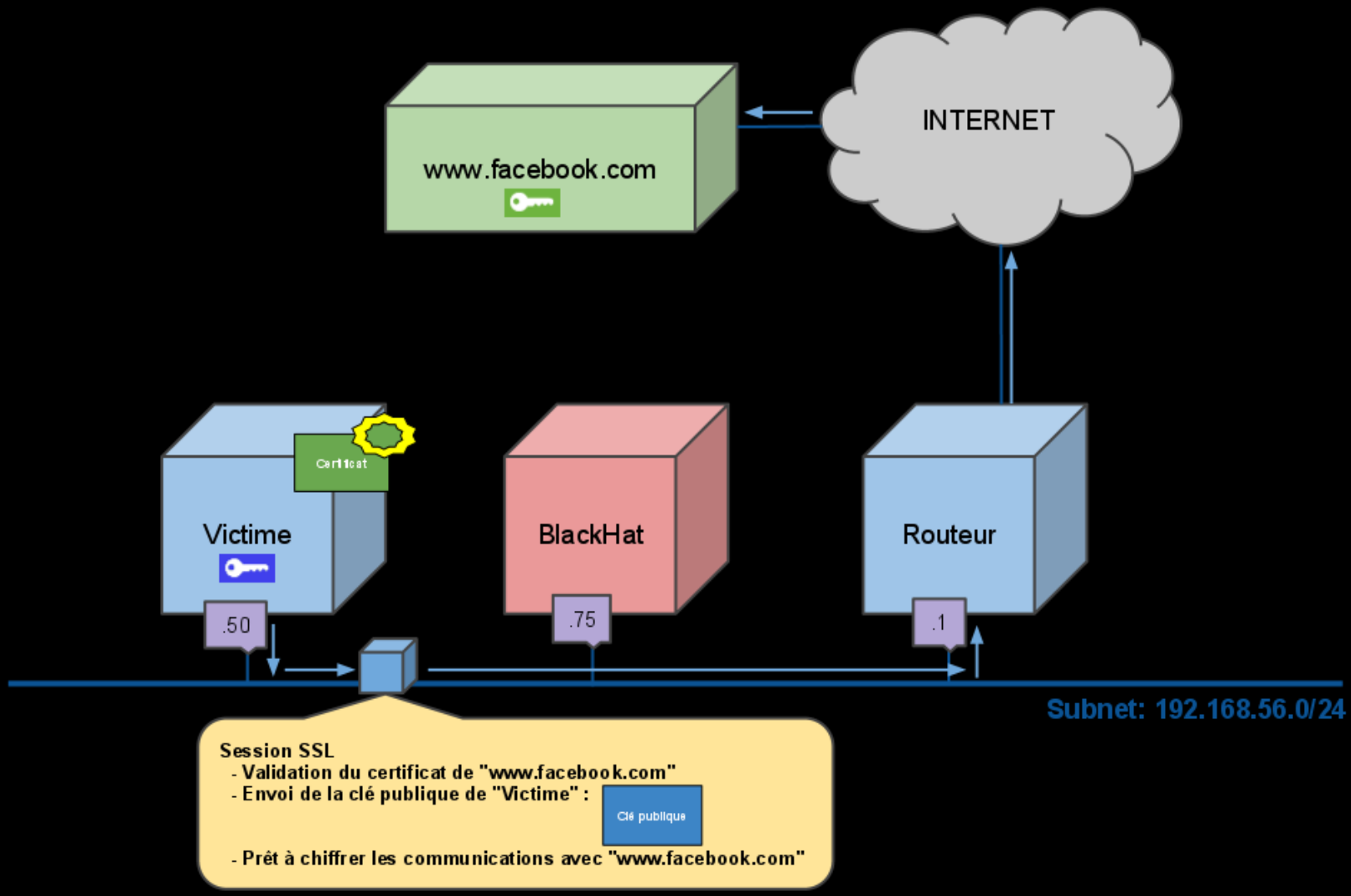
SSL


www.facebook.com
INTERNET
"Victime" veut effectuer une requête http sécurité (https) vers "www.facebook.com"
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Session SSL
- Client Hello

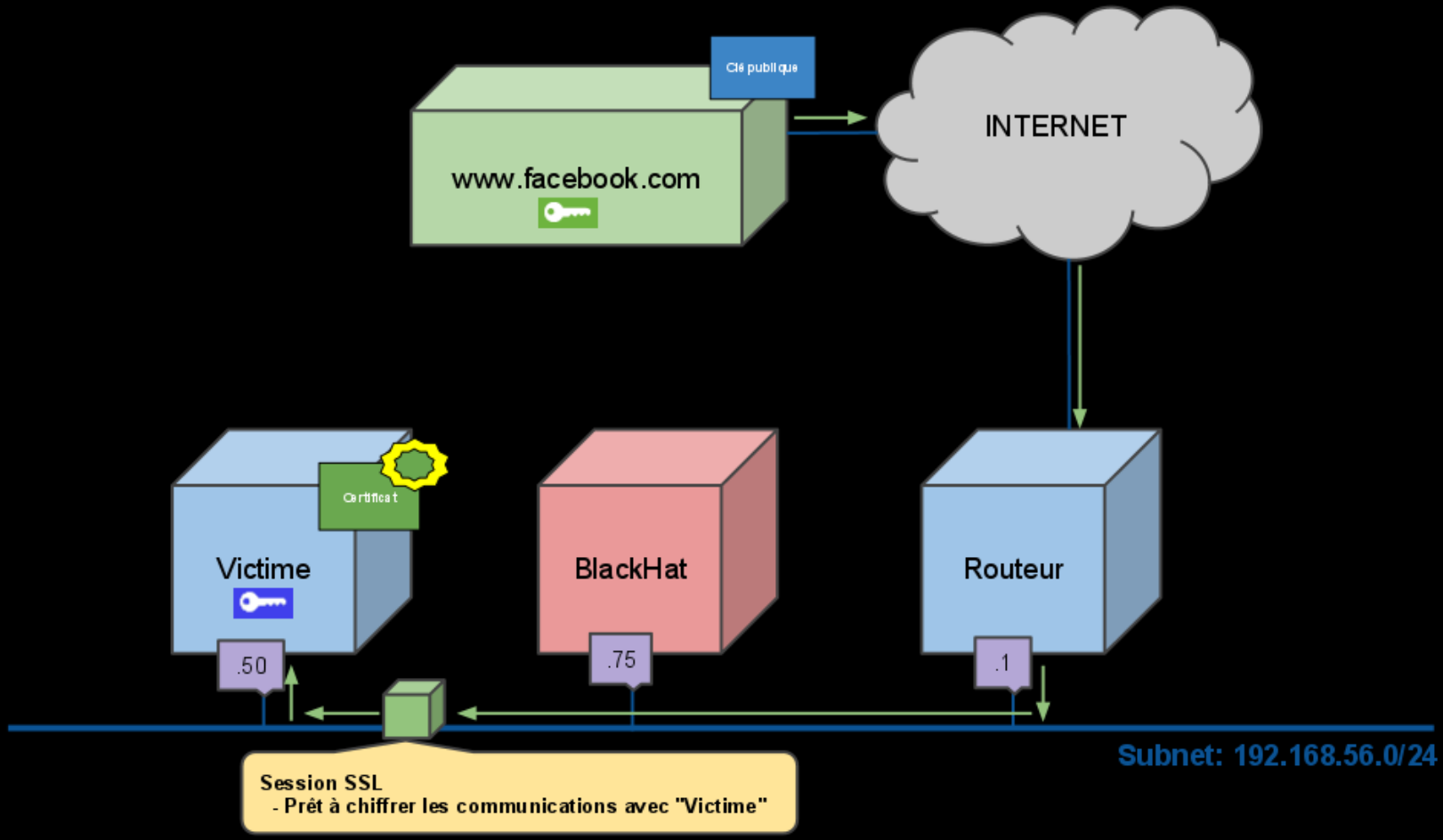
SSL


www.facebook.com
INTERNET
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Session SSL
- Server Hello
- Envoi du certificat de "www.facebook.com":
Certicat

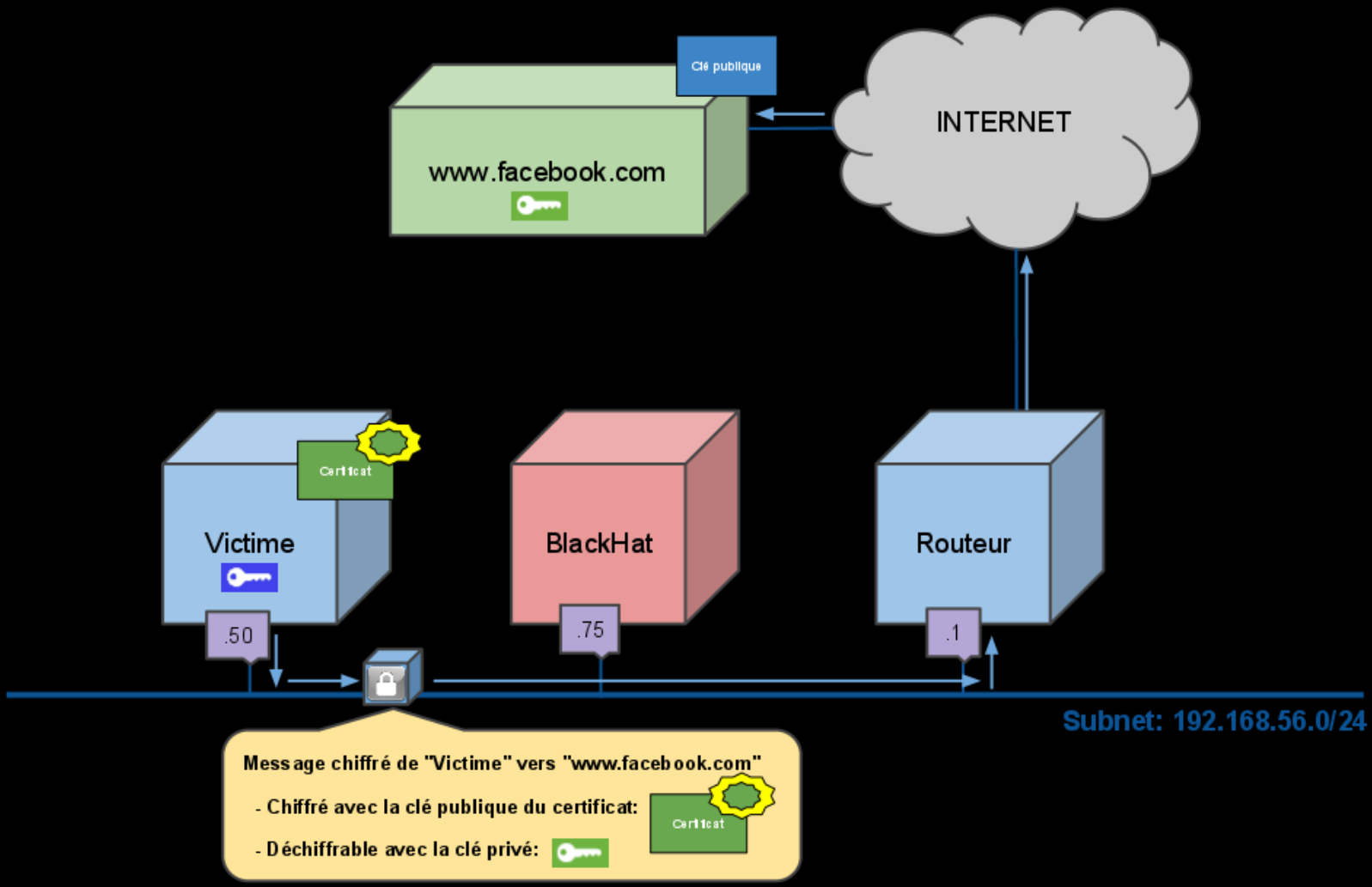
SSL


www.facebook.com
INTERNET
Certificat
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Session SSL
- Validation du certificat de "www.facebook.com"
- Envoi de la clé publique de "Victime" :
Clé publique
- Prêt à chiffrer les communications avec "www.facebook.com"

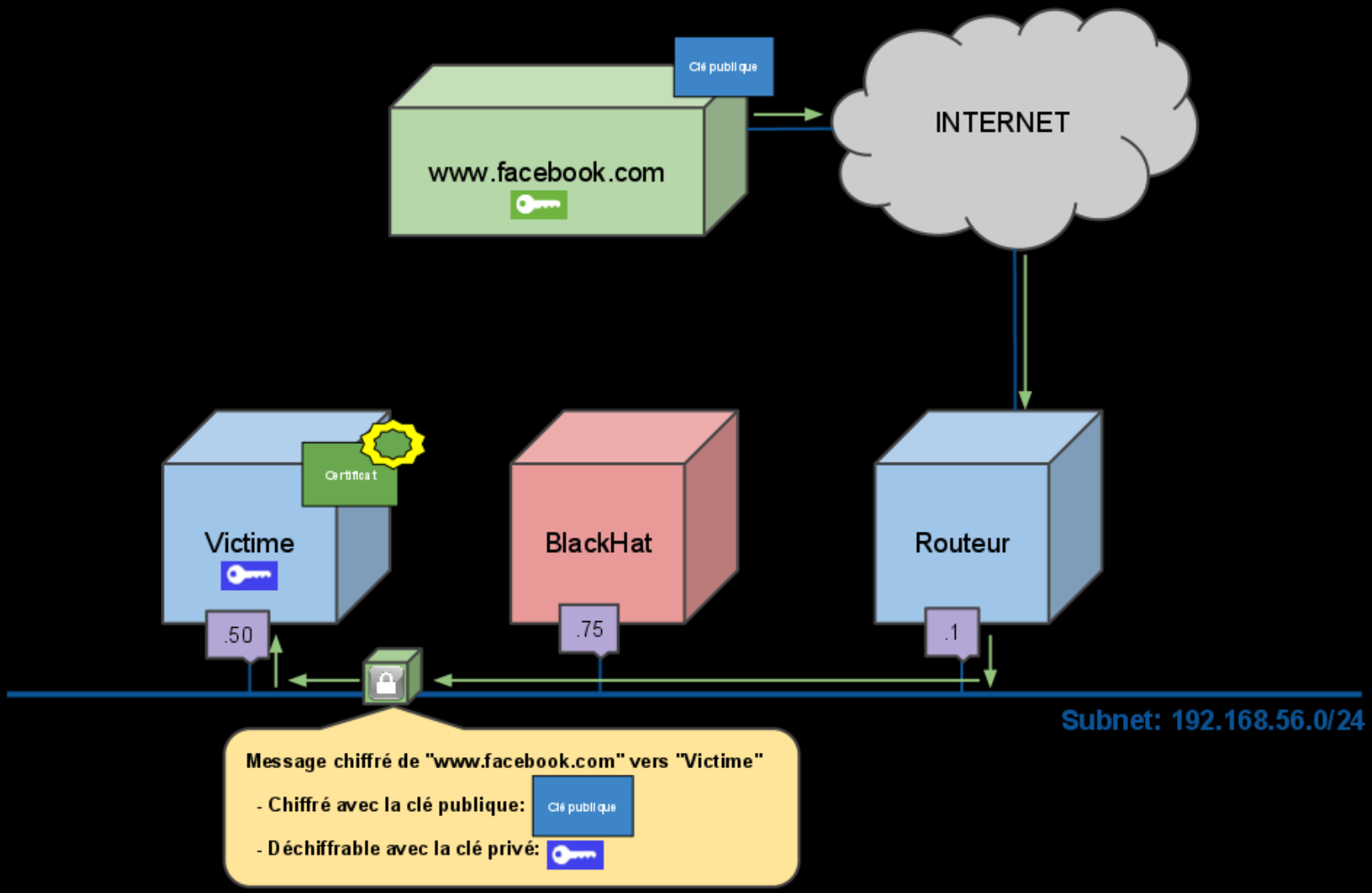
SSL


Clé publique
www.facebook.com
INTERNET
Certificat
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Session SSL
- Prêt à chiffrer les communications avec "Victime"

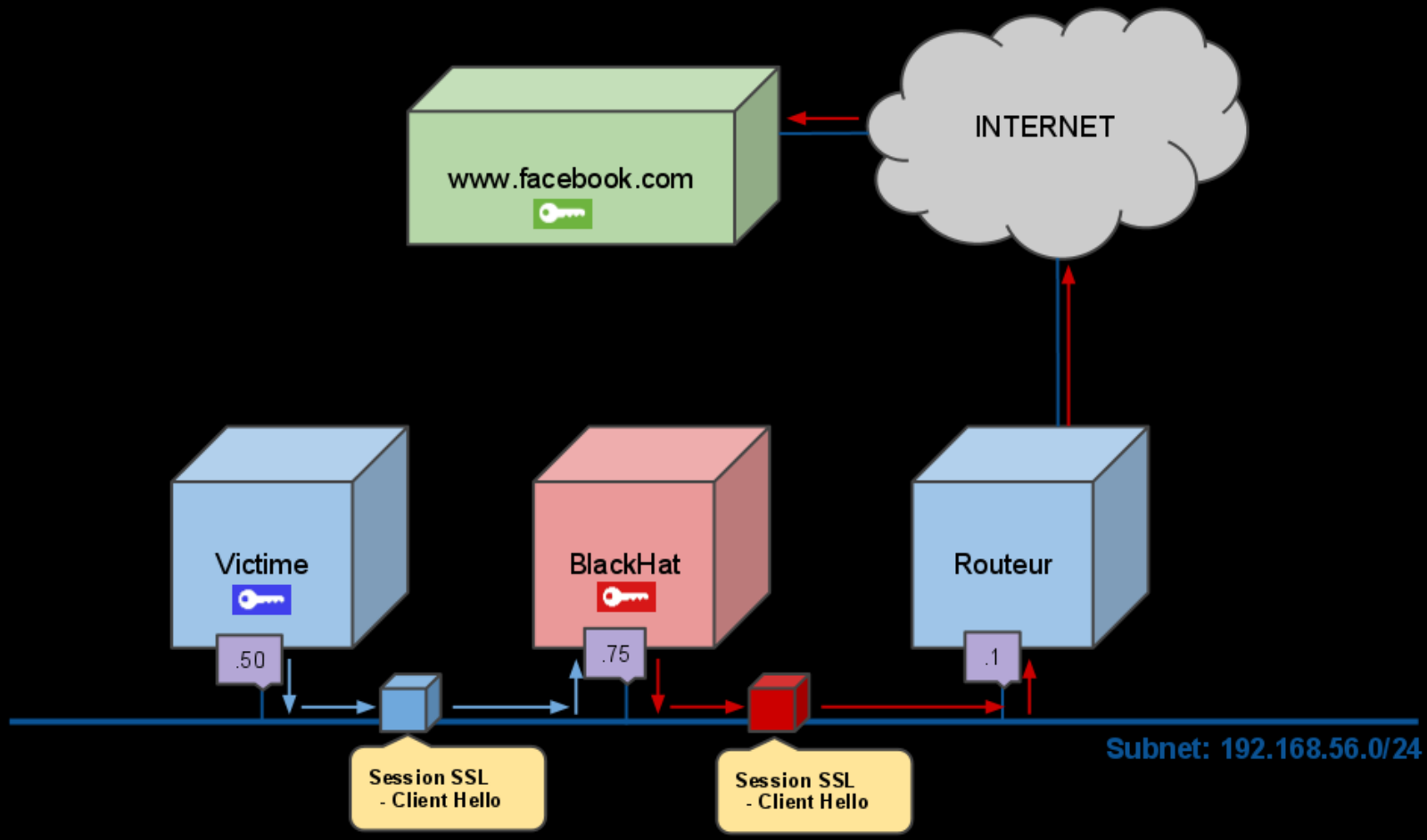
SSL


Clé publique
www.facebook.com
INTERNET
Certificat
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Message chiffré de "Victime" vers "www.facebook.com"
- Chiffré avec la clé publique du certificat:
- Déchiffrable avec la clé privé:
Certificat

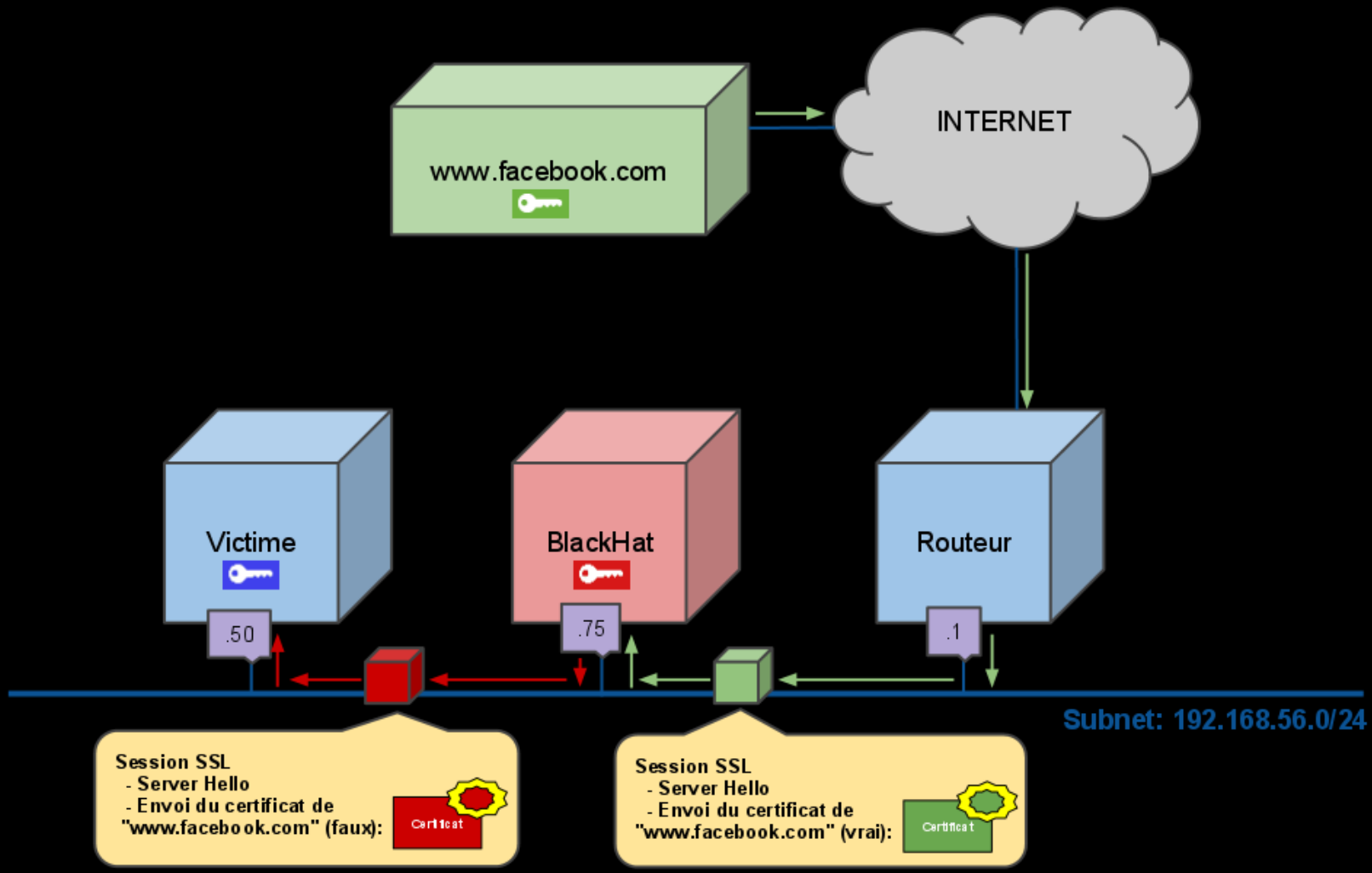
SSL


Clé publique
www.facebook.com
INTERNET
Certificat
Victime
BlackHat
Routeur
.50
.75
.1
Subnet: 192.168.56.0/24
Message chiffré de "www.facebook.com" vers "Victime"
- Chiffré avec la clé publique:
Clé publique
- Déchiffrable avec la clé privé:

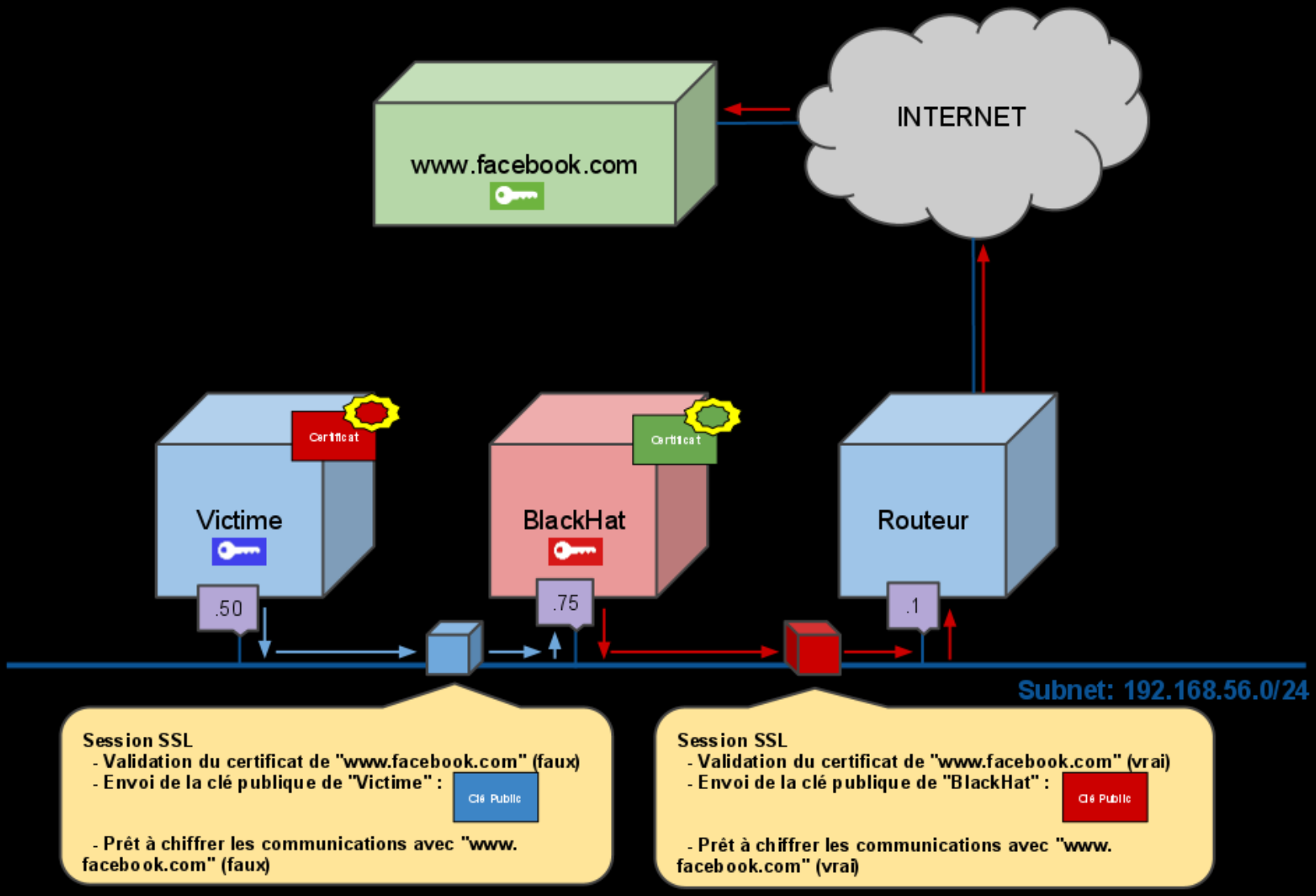
Explications d'un «SSL Splitting »



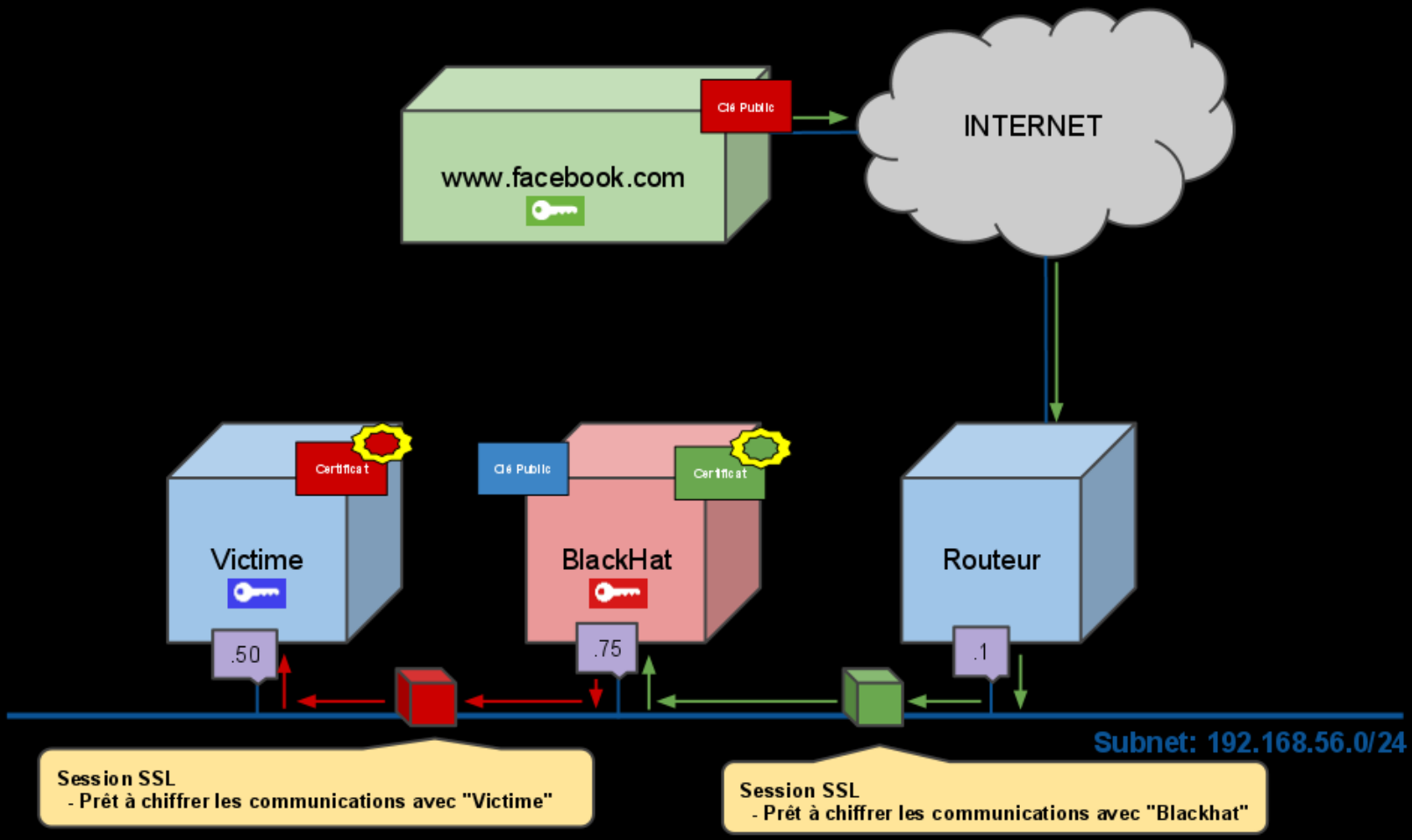
Explications d'un «SSL Splitting »



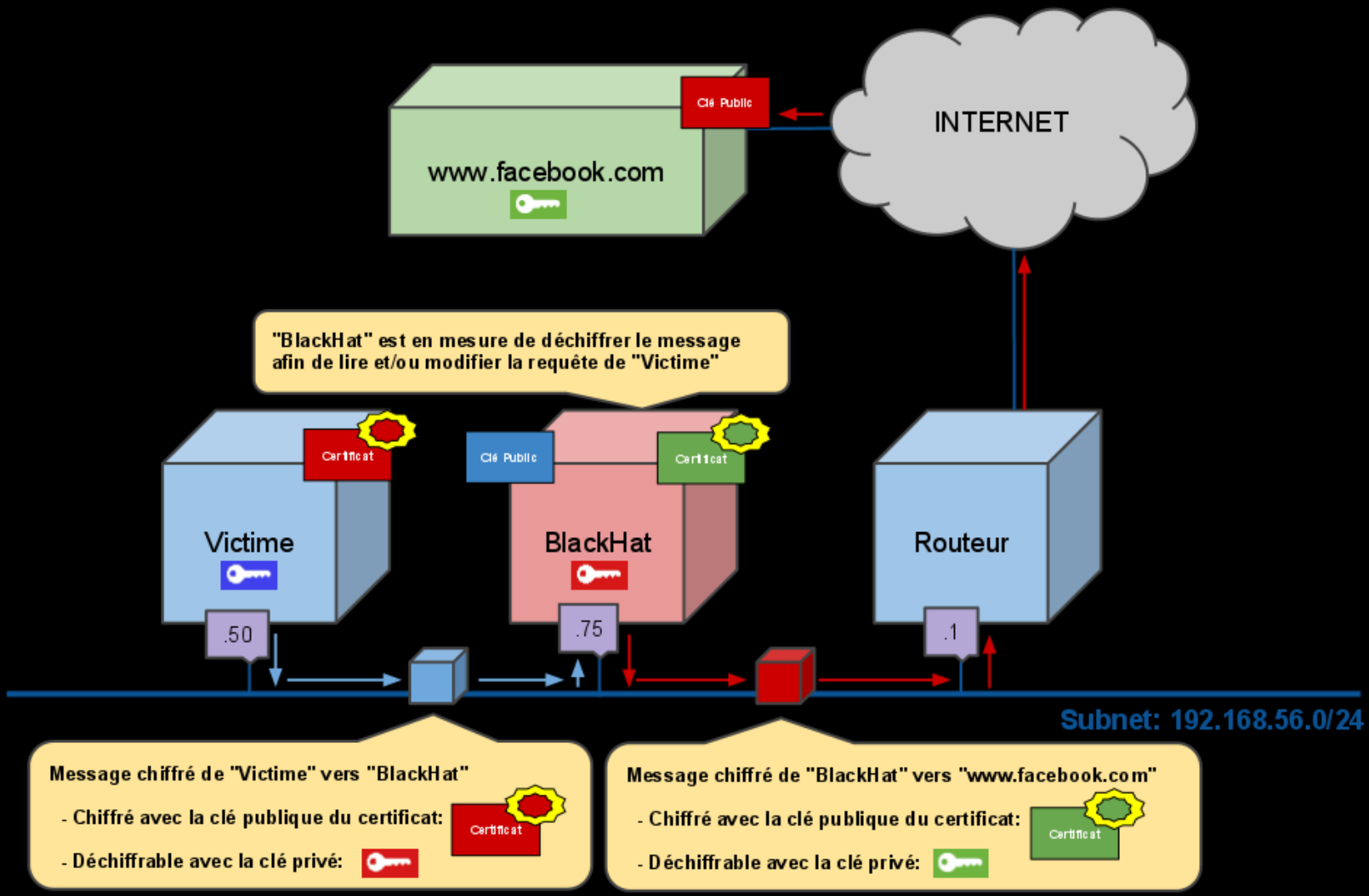
Explications d'un «SSL Splitting »



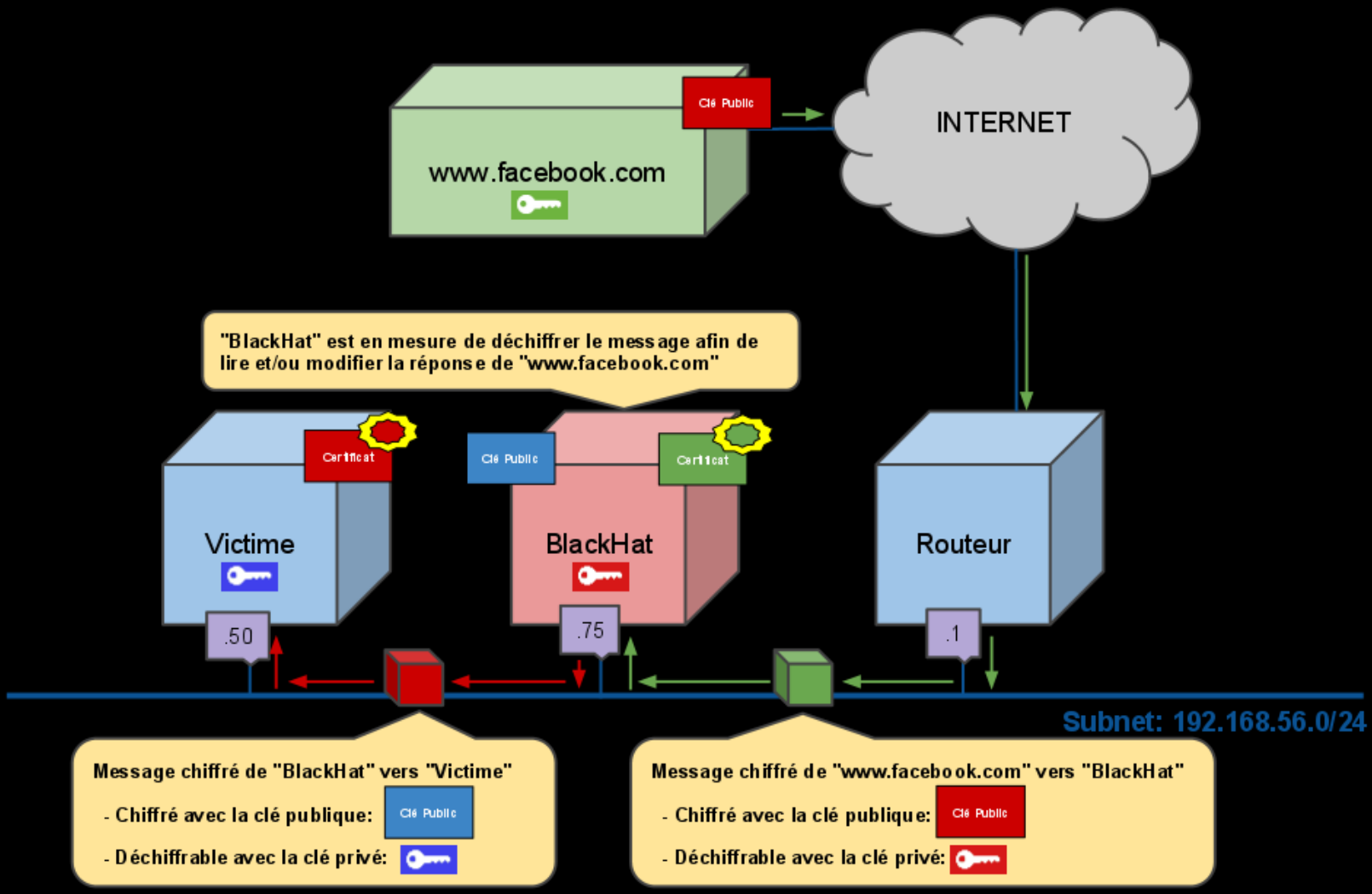
Explications d'un «SSL Splitting »



Explications d'un «SSL Splitting »



Explications d'un «SSL Splitting »



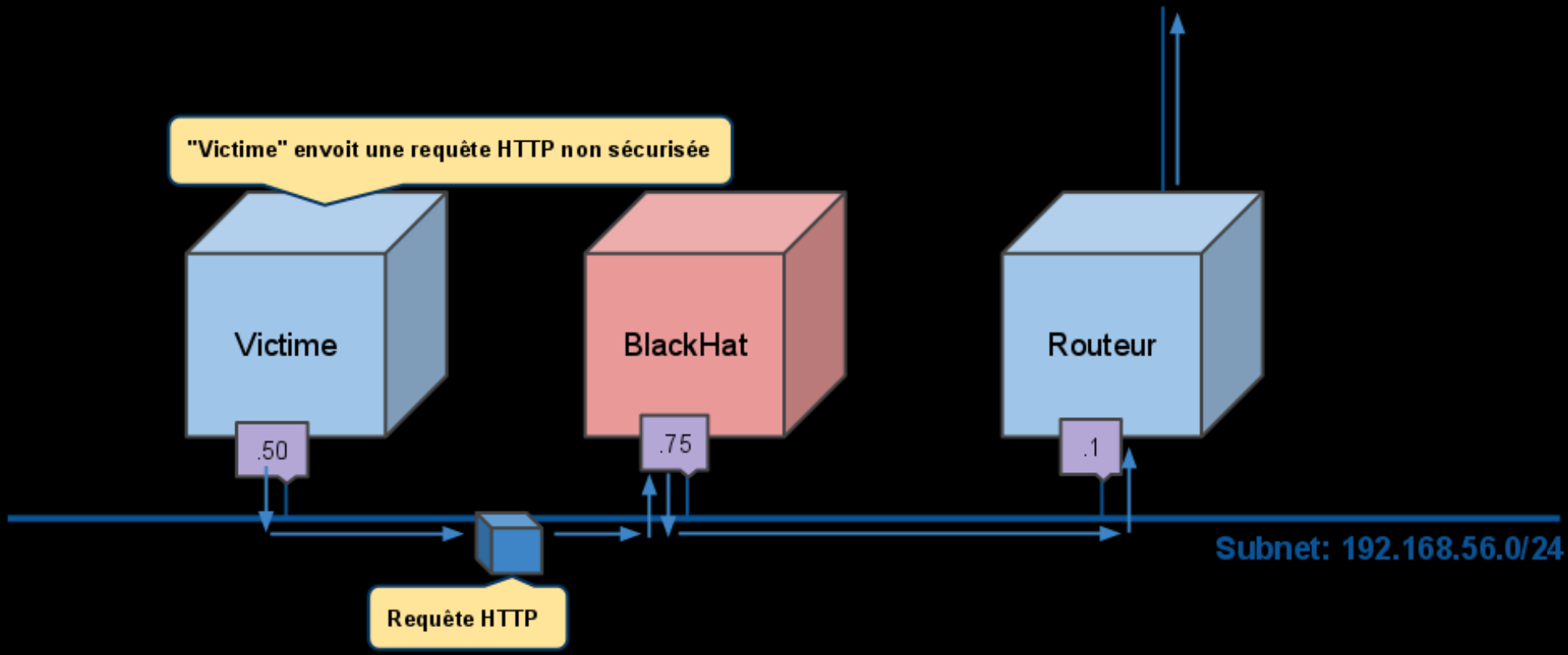
Démo

Attaque #3

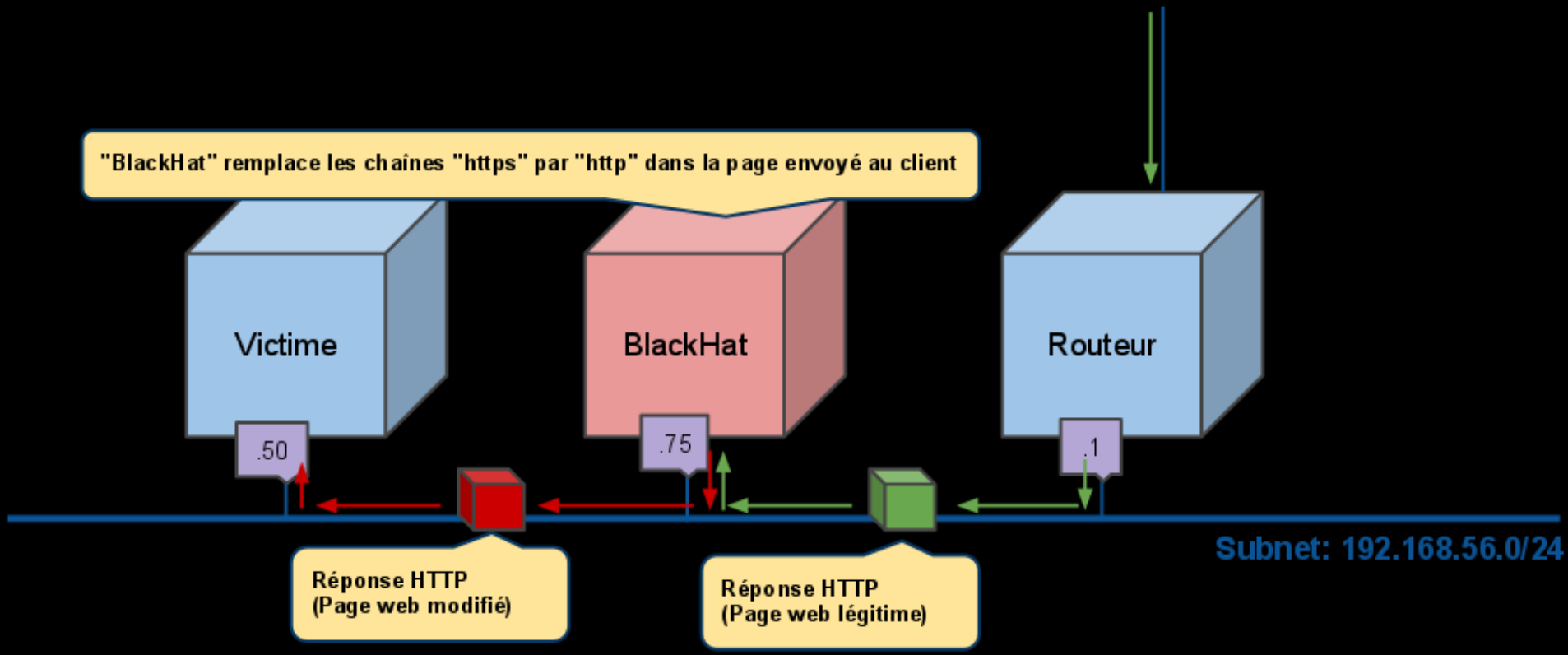
«HTTPS Splitting»

Table des matières

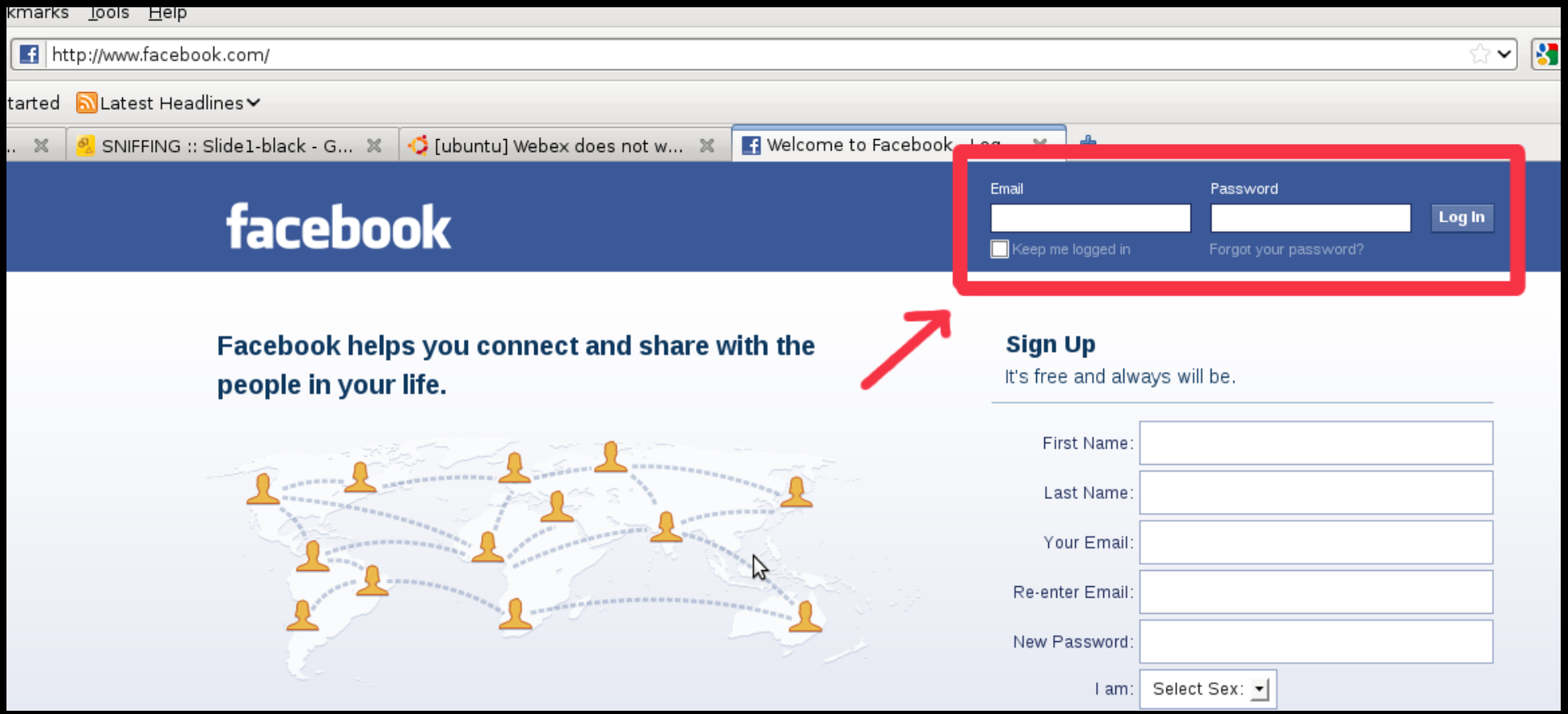
Explications de « HTTPS Stripping »



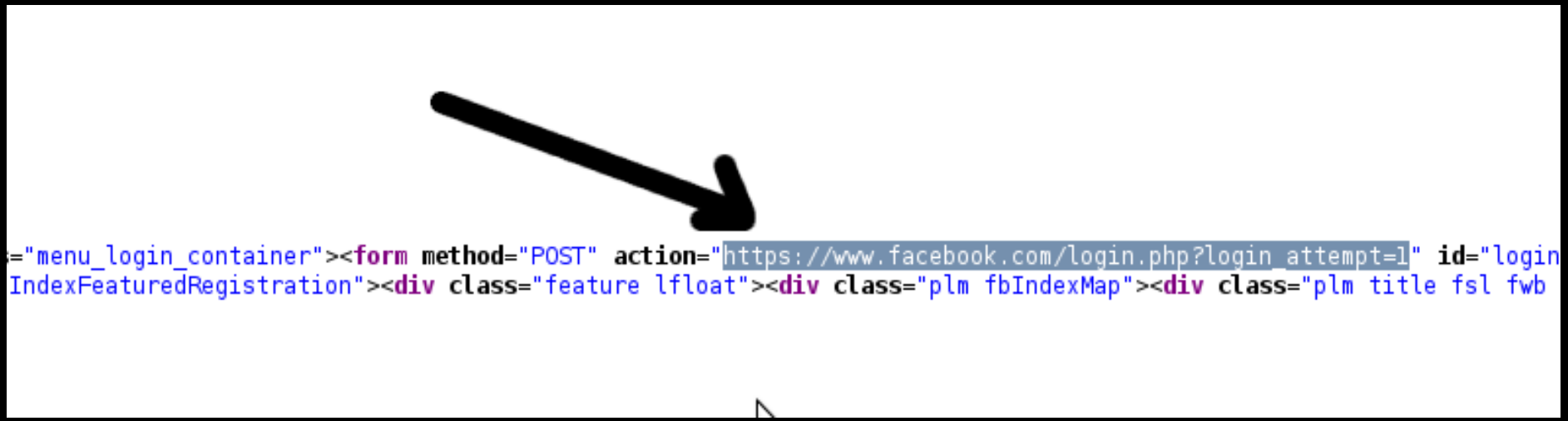
Explications de « HTTPS Stripping »



Explications de « HTTPS Stripping »



Explications de « HTTPS Stripping »



Démo

Attaque #4

«HTTPS Stripping»

Questions?

Merci!