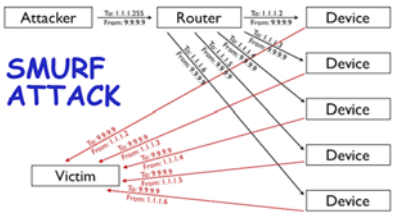
Génierie de Protocoles et Logiciels Sécurisés

Vulnérabilités et Attaques Réseaux

Version 1



Yacine Challal

14/01/2015

Table des matières

Vulnérabilités et attaques réseaux

I

A. Typologie des faiblesses réseaux

Faiblesses réseaux

Les faiblesses des réseaux proviennent essentiellement du fait que les protocoles réseaux n'aient pas été conçus avec prise en compte des problèmes sécuritaires dès le départ. A cela se rajoute les faiblesses issues de l'erreur humaine. Ainsi, on peut classifier les faiblesses réseaux comme suit :

1. **Faiblesses des protocoles :** les protocoles réseaux n'ont pas été conçus pour contrecarrer les attaques de sécurité potentielles, ainsi les protocoles réseau ne s'appuient pas sur une couche "sécurité" et offrent donc plusieurs vulnérabilités
2. **Faiblesses d'authentification :** la majorité des protocoles ne s'appuient sur aucun mécanisme d'authentification. Ceci facilite les attaques se basant sur l'usurpation d'identité comme IP Spoofing
3. **Faiblesses d'implémentation :** certains protocoles sont mal implémentés ou mal programmés ce qui offre certaines vulnérabilités exploitables comme TCP SYN ou Ping-of-the-death
4. **Faiblesses de configuration :** beaucoup d'attaques sont dues à l'erreur humaine qui se manifeste par exemple par une mauvaise configuration, comme une mauvaise configuration d'un pare-feu qui laisse passer un flux non autorisé.

B. Typologie des attaques réseaux

Les attaques réseau peuvent être classées comme suit :

- Attaques de dévoilement du réseau : ont pour objectif de découvrir les artères du réseau (le routage), les machines présentes dans un réseau, les ports ouverts sur un serveur et toutes autres informations pertinentes pour

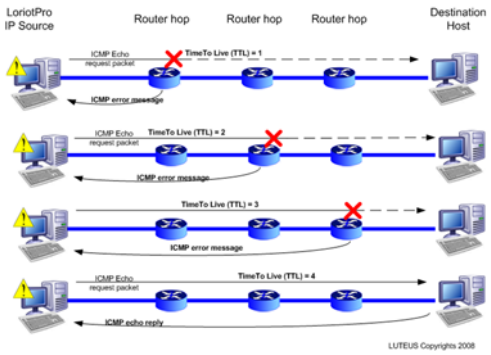
mener une attaque contre un réseau cible.

- Attaques passives d'écoute du trafic : consistent à utiliser un "snifer" pour écouter les échanges dans un réseau. C'est souvent effectué au niveau des couches basses (Ethernet, WiFi, ..) où l'écoute est relativement facilité par la nature broadcast des protocoles. Néanmoins, ce type d'attaque peut être également mené au niveau routage grâce à des attaques de type "Sink hole" où les noeuds malicieux annaoncent des routes courtes vers des destinations prisées pour attirer le flux qui sera lu et analysé par les couches supérieures.
- Attaques d'interférence avec des sessions réseaux : consistent à interférer avec des sessions ouvertes par des entités légitimes puis voler leur session.
- Attaques de déni de service : ont pour objectif de rendre un service ou une machine ou un réseau inopérationnel.
- Attaques de modification du routage réseau : ont pour objectif de détourner des flux afin de les écouter et analyser ou perturber le routage ce qui se traduit généralement par un déni de service
- Attaques indirectes: comme les virus vers qui ont un impact souvent destructif des données sur les cibles et parfois même du matériel. Les chevaux de Troie appartiennent aussi à cette catégorie et sont utilisés pour le vol d'informations.

C. Attaques permettant de dévoiler le réseau

Attaques par cartographie du réseau

Elle permettent de découvrir les artères de communication d'un futur système cible, en utilisant traceroute par exemple. Traceroute utilise l'option TTL du paquet IP pour émettre un message ICMP time_exceeded pour chaque routeur qu'il traverse. La figure suivante illustre une telle attaque. La découverte des routes est une des premières étapes vers une attaque élaborée sur le système cible.

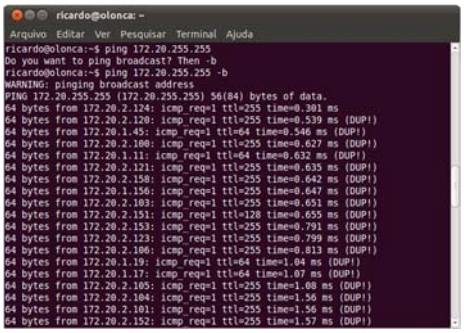


Dévoilement du routage en utilisant traceroute

Attaque par balayge ICMP

Utilisation de ICMP echo-request (ping) pour avoir la réponse du serveur cible (echo-reply) Pour balayer tous les serveurs dans un réseau, on peut envoyer ping à l'adresse broadcast du réseau .

La figure suivante illustre une telle attaque :

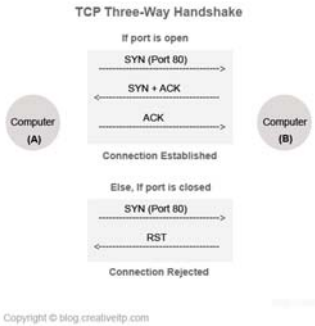


Balayage ICMP

Attaque par balayage TCP

Le client envoie une requête TCP SYN vers une adresse IP et Num POrt, s'il reçois une réponse SYN/ACK alors une application écoute sur le port S'il reçoit RST, ceci signifie qu'aucune application n'utilise ce port.

La figure suivante illustre une attaque par balayage TCP :



Attaque par balayage TCP

D. Attaques permettant d'écouter le trafic réseau

Définition

Cette technique est utilisées pour écouter des informations sensibles comme des mots de passe.

Attaque par Sniffing

Dans un réseau fonctionnant en mode broadcast (le cas de Ethernet) le flux atteint toutes les cartes réseau connectées au réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées Grâce à une table d'écoute (sniffer) il est possible d'intercepter les trames reçues par la carte réseau

Exemple

Un sniffer comme Ethereal ou WinDump/TCPDump ou Wireshark, permet de récupérer tous les paquets IP et analyser leur contenu, qui peut être un paquet TCP contenant un paquet HTTP renferamnt des données HTML.

E. Attaques d'interférence avec une session réseau

1. ARP Spoofing

Rappel : ARP

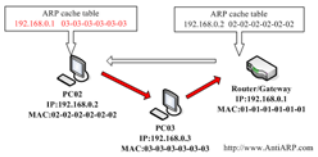
ARP (Address Resolution Protocol) permet de faire la correspondance entre une adresse IP et MAC afin de communiquer avec les systèmes voisins

Attention : Vulnérabilité de ARP

La faiblesse d'authentification de ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. Le Pirate reçoit donc tout le traffic à destination de la passerelle. Il lui suffit d'écouter ou de modifier massivement le traffic et de router ensuite les paquets vers leur véritable destination.

Exemple

La figure suivante illustre une attaque par ARP Spoofing



ARP Spoofing

2. IP Spoofing: falsification d'adresse source IP

Les flux sont parfois traités différemment selon la source: QoS, confiance etc.

Exemple : rsh sous UNIX

Sous UNIX rsh autorise l'exécution de commandes sans authentification si la source est une adresse IP de confiance qui se trouve dans la liste des machines de confiance rhosts

Attention : Vulnérabilité

Il suffit donc pour un pirate de remplacer l'adresse source de ses paquets par une adresse de confiance pour s'octroyer les privilèges.

3. TCP Spoofing

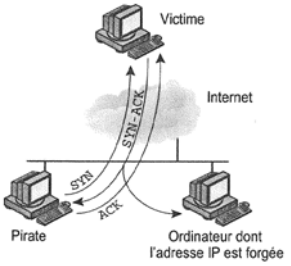
La pirate souhaite ouvrir une session TCP sur une station victime en usurpant l'identité d'une station de confiance. L'attaque se déroule selon les étapes suivantes:

- La pirate analyse le traffic pour connaître l'adresse de la station de confiance autorisée à se connecter au Serveur (Victime)
- Pirate => Serveur: SYN(IP Confiance)
- Pirate rend la station de confiance inopérante pour qu'elle ne réponde pas au Serveur
- Serveur => Station de confiance: SYN/ACK

Puis on distingue deux cas selon que le pirate est sur le même réseau que la station de confiance ou pas.

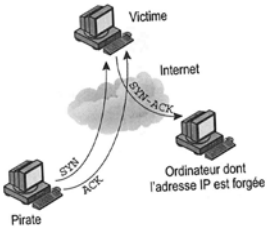
Méthode : Cas où le pirate est sur le même réseau que la station de confiance

- Pirate intercepte SYN/ACK
- Pirate => Serveur: ACK (IP Confiance)



Méthode : Cas où le pirate n'est pas sur le même réseau que la station de confiance (TCP Spoofing aveugle)

Si l'attaquant est sur un autre réseau il ne puurra pas écouter SYN/ACK et ne pourra donc pas connaître l'ISN envoyé par le serveur Il doit donc échantillonner l'algorithme de génération des ISN du serveur en ouvrant quelques connexions légitimes. Si l'algorithme est simple, il pourra deviner le prochain ISN et répondre avec ACK avec le bon numéro .



4. Hijacking (Détournement)

Définition : Hidjacking

La machine du pirate utilise la session engagée entre les deux machines A et B afin que ce soit elle qui soit en session avec la machine B. A perd la session avec B, et la machine du pirate continue la session engagée par A sur B.

Définition : TCP Hidjacking

Le détournement de session TCP permet de rediriger un flux TCP en outre-passant les authentifications nécessaires à l'établissement des sessions (Telnet, FTP, etc.)

Méthode : Etapes d'une attaque TCP Hidjacking

- Phase 1: écouter le traffic avec un sniffer et analyser les messages TCP SYN, ACK et numéros de séquence
- Phase 2: après établissement de la connexion, provoquer une désynchronisation entre les deux machines en répondant à la place de la machine usurpée (Spoofing)
- Phase 3: jouer le rôle de la machine usurpée et détourner la session

Exemple : Hijacking d'une session Telnet

- Pirate sniffe le traffic Telnet (Port TCP 23) entre A et B
- Pirate attend jusqu'à ce que A s'authentifie auprès du service Telnet au niveau de B
- Pirate procède à une désynchronisation de la session entre A et B:
  - Il forge un paquet TCP avec adresse de A (Spoofing) et comme numéro d'acquittement celui attendu par B
  - B accepte ce paquet et permet au Pirate de s'insérer dans la session initialement établie par A .
  - Si A envoie un paquet à B, il n'est pas accepté car ne comporte pas le nuémro de séquence attendu par B

Complément

Pour éviter un ACK storm (A envoie à B et B envoie à A des ACK qui se le refusent à cause de la désynchronisation) le Pirate peut utiliser l'attaque ARP Spoofing vers le système A pour lui indiquer que l'adresse MAC correspondante à l'adresse IP de B est celle du Pirate.

F. Attaques de Déni de Service

1. SYN Flooding

Définition

Consiste à consommer toutes les ressources de la couche TCP d'un ordinateur.

Méthode

Les paquets SYN sont utilisés pour initier les connexions TCP. La machine qui reçoit un SYN répond par un SYN-ACK, à ce moment la connexion est partiellement établit. La machine cible met cette connexion dans une queue de connexions qui attendent un ACK pour compléter le three-way-handshake. Le but de l'attaque est de saturer la queue, de ne jamais envoyer les ACK attendus et ainsi d'empêcher le système d'accépter de nouvelles demandes de connexion.

Complément

L'attaquant peut utiliser dans ses paquet SYN des adresse IP source arbitraire pour rendre l'attaque anonyme.

2. Attaque Smurf

Définition

Consiste à noyer la victime dans un flux de réponses ICMP

Rappel : ICMP

ICMP est un protocole utilisé entre autres pour vérifier qu'une machine est atteignable sur le réseau (ping) Quand une machine reçoit un paquet ICMP echo request, elle envoie un paquet ICMP echo reply à l'adresse IP source indiquée dans le paquet de requête.

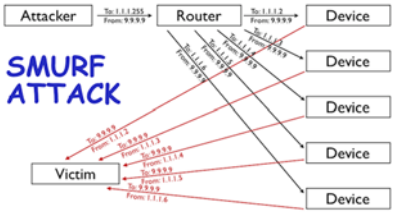
Méthode

Pour attaquer une cible, le pirate inscrit l'adresse de la cible comme adresse source d'un ICMP echo request qu'il envoie à une destination (pour amplifier l'attaque le pirate envoie la requête à une adresse de diffusion)

Exemple

Par convention, une adresse machine dont la représentation ne contient que des 1 est une adresse de diffusion – adresse de diffusion du réseau 10.0.0.0 est 10.255.255.255. Ainsi, toutes les machines de ce réseau envoient une réponse à la victime de l'attaque.

La figure suivante illustre une telle attaque.



Attaque Smurf

3. Distributed Denial of Service (DDoS)

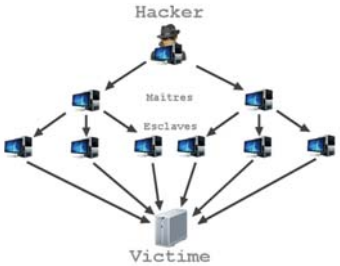
Définition : DDoS

Le DDoS consiste à avoir à ses ordres un grand nombre de machines qui vont simultanément attaquer une seule cible.

Méthode

Le pirate profite d'une vulnérabilité dans le logiciel d'un nombre important de machines pour y installer un client qui s'exécute d'une manière cachée sur les machines infectées. Les machines compromises sont appelées les « bots » (robots) ou des zombies. Ils ne communiquent pas directement avec le Pirate, ils se connectent à un serveur sur lequel se connecte aussi le Pirate (Serveur Chat, P2P, Twitter, ... pour faire communiquer les bots et bostmaster afin de recevoir les ordre d'attaque).

La figure suivante illustre une telle attaque :



DDoS

4. Attaques de modification du routage réseau

Rappel : Routage

Les protocoles de routage ont pour rôle de maintenir des tables de routage Pour cela, les routeurs s'échangent périodiquement des informations de routage (état de

liens, coût de routes, etc.)

Attention : Impact d'une attaque sur le routage

Toute attaque du routage peut impacter la disponibilité du réseau ou permettre le détournement du trafic à des fins de vol d'information

Méthode

Il existe plusieurs attaques selon protocole de routage utilisé. Parmi ces attaques, on peut citer :

- Black hole: un routeur qui annonce des routes qui ne lui appartiennent pas ou avec un coût minimal ! Ceci permet l'attraction de tout le trafic vers cette destination
- Man in the middle: annonce de routes attrayantes pour faire passer le trafic par le pirate puis le router vers la vrai destination
- Numéro de séquence maximal: dans OSPFv2 le num de seq est utilisé pour détecter les annonces obsolètes ou double. Un num seq plus grand est favorisé. Un pirate qui fait une annonce (LSA) avec num seq maximal provoque l'ajustement du routage.

G. Etude de cas : Attaque de Kevin Mitnick

Historique

Il s'agit d'une attaque célèbre perpétrée par Kevin Mitnick contre Tsutomu Shimomura. Kevin était recherché par les autorisé américaine pour le délit commis.

Kevin Mitnick Wanted

Méthode : Trace et attaque

Le fichier suivant contient la trace originale de l'attaque :

Les paquets TCP sont décrits à l'aide de lignes ayant le format suivant:

14:18:37.26 alice.513 > bob.514: P 1382727010(2) ack 2024384001

- 14:18:37.26 l'heure
- Alice: adresse source
- 513 : port source
- Bob: adresse destination
- 514: port destination
- P: un flag éventuel (S=SYN, P=PUSH, F=FIN, R=RESET,, .=pas de flag)

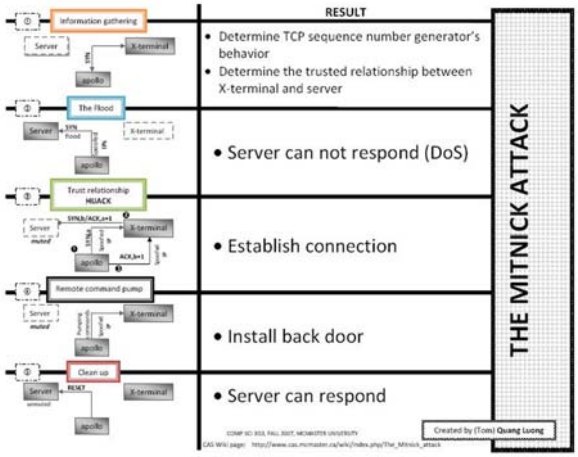
- 1382727010(2): numéro de séquence du premier octet transmis et (2) le nombre d'octets transmis
- ack: éventuel acquittement des octets reçus
- 2024384001: numéro de séquence du prochain octet attendu.

Dans cette trace on reconnaît les étapes suivantes de l'attaque :

- dans un premier temps, Kevin rend la machine de confiance Server inopérante grâce à une attaque de type SYN Flooding.
- Puis, Kevin tente plusieurs connexions à partir d'une machine Appolo sur le serveur x-terminal afin d'échantillonner son algorithme de génération des ISN. En effet, Kevin souhaite se connecter sur x-terminal en usurpant l'identité de la machine de confiance Server (TCP Spoofing) mais il ne se trouve pas sur le même réseau que Server. De ce fait, il aura besoin de l'algorithme de génération des ISN de x-terminal afin qu'il puisse répondre avec le bon ISN quand il enverra le ACK pour confirmer sa demande de connexion TCP sur x-terminal.

  Après cette phase d'échantillonnage, Kevin conclut que la couche TCP de x-terminal rajoute tout simplement 128000 à l'ISN généré lors de la dernière session TCP.
- Kevin ouvre maintenant une session TCP sur x-terminal en usurpant l'identité de la machine de confiance Server. Il en est capable acr il peut répondre avec le bon ACK car il connaît l'ISN qui sera généré par x-terminal dans le SYN-ACK qu'il enverra à Server ; ce sera le dernier ISN + 128000.
- Kevin "upload" des données sur x-terminal. Il s'agit d'une "back door" : des lignes dans un fichier de configuration du service rsh, permettant ainsi à Kevin Mitnick d'avoir accès à la machine cible.
- Kevin annulle les sessions TCP ouvertes sur Server, qui ont provoqué son gel, pour le remettre dans son état opérationnel.
- Kevin peut maintenant se connecter en toute quiétude sur x-terminal sans devoir usurper la machine de confiance Server.

La figure suivante illustre les étapes de l'attaque :



Attaque de Kevin Mitnick

Série d'exercices IV

II

A. IP Spoofing

Avoine et al. 2010

Une attaque d'IP spoofing consiste à se faire passer pour une autre machine en utilisant son adresse IP comme adresse source. La fameuse attaque de Mitnick contre Shimomura avait pour but de faire exécuter une commande malicieuse sur la machine cible en se faisant passer pour une machine se trouvant dans le même réseau local.

Question 1

Pourquoi l'attaquant a-t-il utilisé l'adresse IP d'une machine existante au lieu d'en choisir uen au hasard ?

Question 2

Quelles sont les trois étapes principales de cette attaque ?

Question 3

Si l'attaquant s'était trouvé sur le même réseau local, en quoi l'attaque aurait-elle été différente ?

Question 4

Quelle est la différence entre une attaque de spoofing et une attaque de vol de session au niveau de la couche TCP ?

Question 5

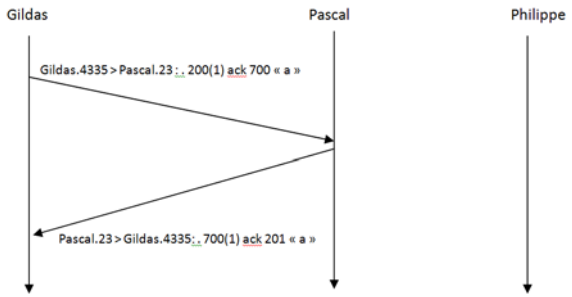
Quel est typiquement le but d'un attaquant qui effectue une attaque de vol de session ?

B. Vol de session TCP

Avoine et al. 2010

Un pirate (Philippe) espioenne une connexion telnet entre Glidas et Pascal. Il forge un paquet TCP pour insérer la commande \n echo HACKED \n dans le flux de

données. Le dernier échange de paquets avant l'insertion est illustré ci-dessous.



Vol de session TCP

Question

Compléter la figure avec le paquet inséré et les paquets suivants.

C. Trafic Réseau Suspect

Avoine et al. 2010

Conrad Ministrateur, un informaticien qui travaille pour une banque suisse, est responsable du bon fonctionnement et de la sécurité du réseau de son employeur. Un matin, lors d'un contrôle de routine, il remarque du trafic suspect à destination du serveur qui gère la base de données des comptes banquaires des clients. Voici un extrait de ce trafic :

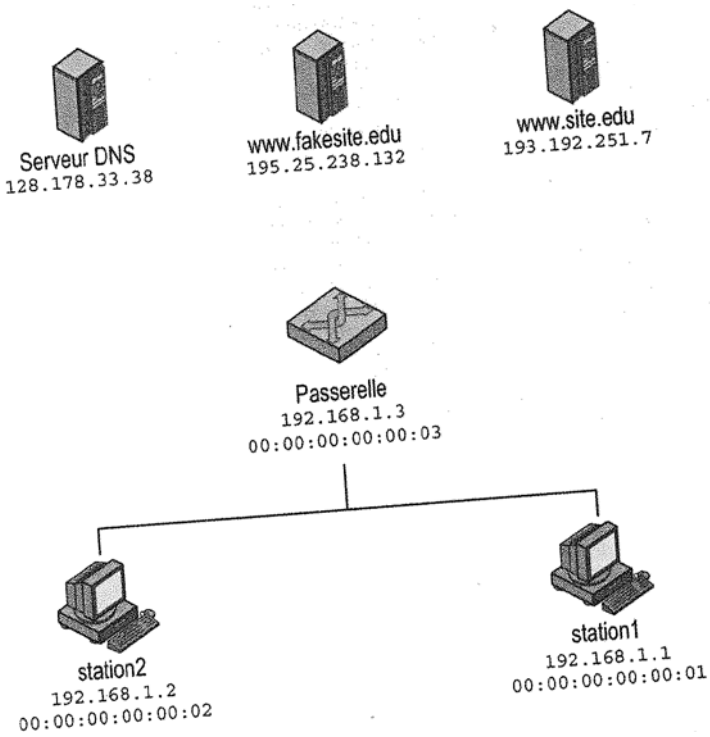
Question

Sachant que l'adresse 192.168. 94.1 est celle de la passerelle qui offre un accès à Internet à ce serveur, interpréter ce trafic de manière concise.

D. ARP / DNS Spoofing

Avoine et al. 2010

On considère un réseau local composé de deux stations de travail et séparé de l'extérieur par un routeur (passerelle). Les stations de travail sont configurées pour utiliser le serveur DNS 128.178.33.38 extérieur au LAN et n'utilisent pas de cache DNS interne. On considère enfin deux serveurs HTTP extérieurs au LAN, www.site.ch et www. fakesite.ch. Les différents éléments sont représentés sur la figure suivante.



Architecture du réseau

L'objectif de l'exercice est de proposer une attaque fondée sur le DNS spoofing, telle que lorsque l'utilisateur de station1 (victime) tentera d'accéder au site www.site.ch, il aboutira de manière transparente sur le site www.fakesite.ch. L'attaque sera effectuée à partir de station2.

Lorsqu'une station souhaite communiquer avec l'extérieur du LAN, elle utilise, comme adresse MAC destination, l'adresse MAC de la passerelle. La passerelle reçoit le paquet et le retransmet en direction de sa destination (qui se trouve en dehors du LAN) ; l'adresse destination dans le paquet IP reste inchangée, on suppose pour l'instant qu'aucune des machines du LAN (y compris la passerelle) ne connaît les adresses MAC des autres machines et que le protocole ARP est utilisé pour obtenir des adresses MAC.

Question 1

L'utilisateur de la machine station1exécute la commande ping 192.168.1.2. Ci-dessous figurent les messages échangés sur le LAN jusqu'à l'envoi du ping ainsi que les adresses contenues dans le paquet ping ; compléter le tableau.

1. 192.168.1.1 envoie [ARP who-has ? 192.168.1.2] à l'ensemble du LAN.
2. 192.168.1.2 répond [ARP is-at 00 :00 :00 :00 :00 :02] à 00 :00 :00 :00 : 00 :01.
3. 192.168.1.1 envoie le paquet à 192.168.1.2

Adresse destination dans le paquet ping	
IP destination	
MAC destination	

Table1

Question 2

L'utilisateur de station1 exécute la commande ping 128.178.33.38 (machine extérieure au LAN). De la même manière que précédemment, indiquer les messages échangés sur le LAN jusqu'à l'envoie du ping, et compléter le tableau :

Adresse destination dans le paquet ping	
IP destination	
MAC destination	

Table2

Bien que les protocoles DNS et ARP soient fondés sur des principes radicalement différents, leur objectif est le même, à savoir éviter à l'utilisateur la mémorisation d'adresses. Le protocole DNS effectue la conversion entre les noms de domaine, en général faciles à retenir, et les adresses IP. On notera [DNS who-is ? <domain name>] une requête DNS et [DNS is-at <IP address>] une réponse DNS.

Question 3

L'utilisateur de station1 exécute la commande ping www.site.ch. Indiquer tous les messages échangés sur le LAN jusqu'à l'envoi du paquet ping, puis compléter les tableaux suivants :

Adresse destination dans la requête DNS	
IP destination	
MAC destination	

Adresse destination dans le paquet ping	
IP destination	
MAC destination	

Table3

Question 4

On suppose maintenant que les machines conservent en mémoire les adresses MAC récemment utilisées. Sachant que de nombreux systèmes d'exploitation acceptent les réponses ARP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment station2 peut se faire passer pour la passerelle auprès de station1.

Question 5

L'utilisateur de station1 exécute la commande ping 128.178.33.38 ; compléter le tableau ci-dessous avec les informations qui seront contenues dans le paquet ping, dans le cas où il n'y a pas d'attaque et dans le cas où l'attaque a lieu.

Adresse destination dans le paquet ping		
	sans attaque	avec attaque
IP destination		
MAC destination		

Table 4

Question 6

On suppose que station2 réussit à se faire passer pour la passerelle auprès de station1. Expliquer comment utiliser cette mascarade pour réaliser l'attaque initialement souhaitée, à savoir que lorsque l'utilisateur de station1 tentera d'accéder au site ww.site.ch, il aboutira de manière transparente sur le site www.fakesite.ch. Il est important de noter que l'attaque doit rester transparente pour station1.

Question 7

On suppose que station2 a mis son attaque en oeuvre. dessiner sur la figure du début de cet exercice les chemins pris par les paquets transitant sur le LAN lorsque station1 exécute la commande ping www.site.ch (on ne dessinera pas les requêtes et réponses ARP).

```
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```