M2 informatique parcours GLIA **Année :** 2024-2025
Durée : 1h30 (hors tiers temps)
Consignes : tous les documents sont interdits ; tous les appareils électroniques (téléphones, calculatrices, ordinateurs, montres connectées) sont interdits

Examen d'administration réseau – première session

Exercice 1 – DHCP (6 points)

Question 1.1 (1 point) : Rappelez à quoi sert le protocole DHCP (Dynamic Host Configuration Protocol).
Question 1.2 (2 points) : Dans le protocole DHCP, un client qui se connecte sur le réseau envoie un message DISCOVER pour identifier les serveurs DHCP du réseau, reçoit un message OFFER de chaque serveur, envoie un message REQUEST au serveur de son choix, et reçoit un message ACKNOWLEDGE. Pour chacun de ces messages : indiquez l'adresse MAC source, l'adresse MAC destination, l'adresse IP source, et l'adresse IP destination. Pour rappel : 0.0.0.0 désigne l'adresse IP d'une machine sans adresse IP.
Question 1.3 (1 point) : Il existe trois types d'allocation d'adresses : l'allocation statique (basée sur l'adresse MAC), l'allocation dynamique (aléatoire) et l'allocation dynamique (initialement aléatoire, puis basée sur l'adresse MAC). Donnez un exemple de cas d'usage pour chacun de ces types.
Question 1.4 (1 point) : Lorsque l'on utilise le NAT (traduction d'adresses), il est déconseillé d'attribuer aux serveurs publics du réseau privé des adresses aléatoires. Pourquoi ?
Question 1.5 (1 point) : Un client se voit attribuer une adresse IP par DHCP pendant une période déterminée au travers d'un bail. Quand la période a besoin d'être étendue, le client en fait la demande au serveur avant la fin du bail, et non pas après la fin du bail. Pourquoi ?

Exercice 2 – Algorithme de Karn dans TCP (6 points)

L'algorithme de Karn [1] est utilisé dans TCP pour estimer le temps d'aller-retour des paquets.

Question 2.1 (1 point) : Pourquoi est-il important dans TCP d'estimer le temps d'aller-retour des paquets ? Indice : pensez à la manière dont la garantie de livraison est implémentée.
Question 2.2 (1 point) : Pourquoi le calcul du temps d'aller-retour est ambigu lorsqu'il concerne des paquets retransmis ?
Question 2.3 (1 point) : Expliquez en quoi l'algorithme de Karn a du mal à adapter le temps d'aller-retour des paquets lorsque le délai de communication augmente brutalement.
Question 2.4 (1 point) : Pour résoudre le problème précédent, l'algorithme de Karn propose d'initialiser un timer de retransmission avec une durée T_0, et de doubler ce timer à chaque retransmission. Montrez en quoi cette solution corrige le problème.
Question 2.5 (1 point) : Quand est-ce que a durée du timer est-elle réinitialisée à T_0 ?
Question 2.6 (1 point) : Est-ce que le temps d'aller-retour intègre les 200ms des acquittements retardés ?

Exercice 3 – Analyse d'attaques récentes (8 points)

Dans cet exercice, nous allons nous concentrer sur des articles de la presse décrivant des attaques de sécurité récentes. Les réponses ne doivent pas se limiter à la traduction des articles, et doivent être justifiées par des éléments techniques.

<< Amplification attacks are one of the most common distributed denial of service (DDoS) attack vectors. These attacks are typically categorized as flooding or volumetric attacks, where the attacker succeeds in generating more traffic than the target can process, resulting in exhausting its resources due to the amount of traffic it receives. (…) Reflection attacks involve three parties: an attacker, a reflector, and a target. The attacker spoofs the IP address of the target to send a request to a reflector (e.g., open server, middlebox) that responds to the target (…). For the attack to be amplified the response should be larger than the request, resulting in a reflected amplification attack. The attacker's motivation is to create the largest reflection out of the smallest requests. Attackers achieve this goal by finding many reflectors and crafting the requests that result in the highest amplification. >>
Source : https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/?msockid=3afff8987499647a0cefec1075aa65b1 (consultation : 12/11/2024)

Question 3.1 (1 point) : Pourquoi les pirates mènent-ils des attaques de type DDoS ?
Question 3.2 (1 point) : Pourquoi voit-on plus souvent des attaques de type DDoS, plutôt que des attaques DoS *(Denial of Service)* ?
Question 3.3 (1 point) : Pourquoi est-ce qu'un pirate cherche à utiliser une technique d'amplification, et non pas à envoyer directement des requêtes à une victime ?
Question 3.4 (1 point) : Comment le pirate cache-t'il le fait qu'il est en train de mener une attaque d'amplification ?
Question 3.5 (1 point) : L'article indique « *The attacker spoofs the IP address of the target* ». Est-ce que c'est simple à réaliser au niveau IP ? Au niveau TCP ?

<< Beginning in 2016, NETSCOUT ASERT observed adversary's launching DDoS attacks towards entire CIDR blocks, rather than individual IP addresses. This phenomena is known as a Carpet-Bombing (Spread Spectrum, Subnet DDoS) DDoS attack. This targeting methodology was intended to make it more challenging for defenders to detect and classify incoming DDoS attacks, as some DDoS defense systems relied solely upon packets-per-second (pps) and/or bits-per-second (bps) thresholds set for specific hosts to detect inbound DDoS attack traffic. >>
Source : https://www.netscout.com/blog/asert/carpet-bombing (consultation : 12/11/2024)

Question 3.6 (2 points) : Décrivez (sans vous contenter de traduire) ce qu'est la méthode du « *carpet bombing* ».
Question 3.7 (1 point) : Proposez une solution pour identifier ces attaques.