M2 informatique (IDL) parcours GLIA, UE administration réseau
Année : 2023-2024 **Durée :** 1h30
Consignes : documents et outils électroniques interdits

Examen d'administration réseau – deuxième session

Exercice 1 : Adressage IP (7 points)

Question 1.1 (2 points) : Identifiez les équipements IP de la figure 1, et donnez leur des adresses IP. Vous utiliserez des numéros de réseaux de classe A (ex : 10.0.0.0/8).
Question 1.2 (2 points) : Indiquez les arbres construits par le protocole du *spanning tree*.
Question 1.3 (2 points) : Indiquez la table de routage des routeurs 1 et 6.
Question 1.4 (1 point) : Indiquez le chemin suivi par les données allant de A à H.

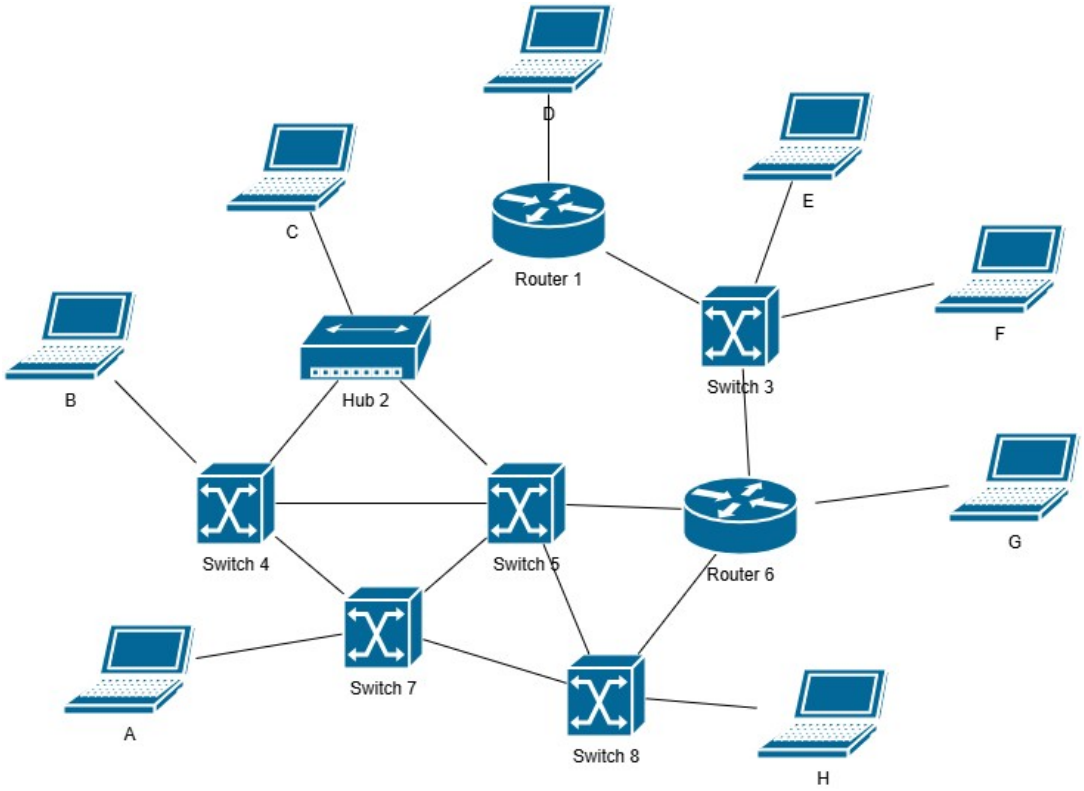

Figure 1 : Un réseau d'entreprise avec 2 routeurs, 1 hub, 5 switchs, et 8 ordinateurs.

Exercice 2 : Administration réseau (3 points)

Question 2.1 (1 point) : Comment fonctionne le protocole DHCP *(Dynamic Host Configuration Protocol)*, et à quoi sert-il ?
Question 2.2 (1 point) : Comment fonctionne le protocole DNS *(Domain Name System)*, et à quoi sert-il ?
Question 2.3 (1 point) : Comment surveiller le trafic d'un réseau pour détecter des problèmes ou des intrusions ?

Exercice 3 : TCP (4 points)

Question 3.1 (1 point) : Comment fonctionne, et à quoi sert la fenêtre d'émission de TCP ?
Question 3.2 (1 point) : Les acquittements sélectifs de TCP (appelés SACK), non étudiés en cours, permettent d'acquitter des segments qui sont reçus hors séquence. Quel est l'intérêt des SACK par rapport aux ACK classiques de TCP ?
Question 3.3 (1 point) : Pourquoi l'estimation du temps d'aller-retour des paquets est importante dans TCP ?
Question 3.4 (1 point) : L'algorithme de Karn propose de calculer le temps d'aller-retour des paquets TCP en ignorant les paquets retransmis. Pourquoi ignore-t'il ces paquets ?

Exercice 4 : Discussion sur des attaques de sécurité de 2024 (7 points)

Cet exercice cite quelques articles détaillant des attaques de sécurité de 2024. L'objectif n'est pas de se positionner par rapport à la véracité de ces faits, mais plutôt de commenter les éléments techniques contenus dans la description. Il ne faut pas se limiter à traduire le texte.
Source : https://www.crn.com/news/security/2024/10-major-cyberattacks-and-data-breaches-in-2024-so-far (auteur : Kyle Alspach, dernière consultation : le 10 juillet 2024).
Remarque préliminaire : vous pouvez demander la traduction des mots anglais inconnus.

Question 4.1 (3 points) : « In January, Microsoft disclosed that a Russia-aligned threat actor was able to steal emails from members of its senior leadership team as well as from employees on its cybersecurity and legal teams. (…) In June, Microsoft confirmed that it had sent out more notices to customers impacted by the compromise, which were notified that their emails were viewed. "This is increased detail for customers who have already been notified and also includes new notifications," the company said in a statement. The breach, which is believed to have begun in November 2023, saw hackers initially gain access by exploiting a lack of MFA (multifactor authentication) on a "legacy" account, Microsoft said. »

- Décrivez l'attaque.
- Quelle est la solution adoptée par Microsoft ?
- Proposez un mode opératoire pour une solution à plus long terme.

Question 4.2 (2 points) : « The FBI said in February that a China-linked threat group was found to have hijacked "hundreds" of small office/home office (SOHO) routers based in the U.S. as part of a campaign to compromise U.S. critical infrastructure providers. (…) The routers compromised by the group together formed an assembly of malware-infected devices, known as a botnet, which the threat group could use for launching an attack against U.S. critical infrastructure, the FBI said. »

- Décrivez l'objectif de l'attaque.
- Expliquez pourquoi l'attaque est particulièrement simple à mettre en place ?

Question 4.3 (2 points) : « In March, Red Hat and CISA warned that the two latest versions of XZ Utils, a widely used set of data compression tools and libraries in Linux distributions, were found to have been compromised. (…) As disclosed by the original maintainer of the XZ Utils project, a contributor to the XZ Utils was responsible for the insertion of malicious code. (…) A Microsoft engineer, Andres Freund, said in a post that he discovered the vulnerability after noticing "odd" behavior in installations of Debian, a popular Linux distribution—including that logins were taking longer and using more CPU than usual.

Security researchers credited Freund with going the extra mile to hunt down the issue, ultimately revealing the backdoor in the software. »

- Commentez l'attaque.
- Commentez la manière dont l'attaque a été trouvée.