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

Examen d'administration réseau – première session

Exercice 1 : *Spanning tree* et adressage IP (6 points)

La figure 1 représente un réseau d'entreprise.

Question 1.1 (3 points) : Le réseau comporte trois réseaux IP : 10.0.0.0/8 (en haut), 20.0.0.0/8 (au milieu) et 30.0.0.0/8 (en bas). Donnez des adresses IP à chacun des équipements IP de la figure.
Question 1.2 (2 points) : Indiquez les arbres construits par le protocole du *spanning tree*.
Question 1.3 (1 point) : Indiquez le chemin suivi par les données allant de ED1 à ED3.

Exercice 2 : TCP (4 points)

Question 2.1 (1 point) : A quoi sert l'algorithme de Nagle dans TCP, et quand faut-il l'activer ?
Question 2.2 (1 point) : Quelle est la définition d'un protocole fonctionnant en mode connecté, comme TCP ?
Question 2.3 (2 points) : Détaillez l'algorithme utilisé par TCP lorsqu'un paquet est reçu. Notez que ce paquet peut être un paquet qui n'est pas reçu dans l'ordre.

Exercice 3 : Discussion sur des attaques de sécurité de 2023 (10 points)

Cet exercice cite quelques articles détaillant des attaques de sécurité de 2023. Les articles sont souvent écrits de manière subjective, et les faits décrits ne sont pas nécessairement prouvés. L'objectif ici 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. Tous les exemples de cet exercice viennent de la page web suivante :
Source : https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2023/
(auteur : Patrick O'Connor, dernière consultation : le 19 décembre 2023).

Remarque préliminaire : vous pouvez demander la traduction des mots anglais inconnus.

Question 3.1 (3 points) : << With so many businesses appreciating the flexible benefits of cloud deployment, cloud providers have grown significantly in the past five years. However, all that computing resource has also attracted criminals who seek to exploit these vast oceans of processing power for their own ends. To entice potential customers, cloud providers often offer free periods to verify their functionality. Criminal groups seek to profit by using such free offers to mine cryptocurrencies. This is often called 'free jacking' as groups will often sign up with fake IDs and stolen credit cards, enabling them to continue past the free period and ramp up their operation until the first bill becomes due or their stolen credit card becomes useless. Also, since often these trials are for short periods, the groups employ quite sophisticated continuous integration/continuous deployment (CI/CD) techniques along with containerisation and other popular DevOps techniques with automation to the fore. >>

- Détaillez l'attaque décrite dans la première partie de cet extrait, jusqu'à « becomes useless. »
- Détaillez la deuxième partie de cet extrait, à partir de « Also, since often », sans vous contenter de la traduire. Pourquoi les attaquents utilisent-ils des techniques sophistiquées d'intégration continue / de déploiement continu ?
- Proposez deux solutions pour détecter ou empêcher ce type d'attaques.

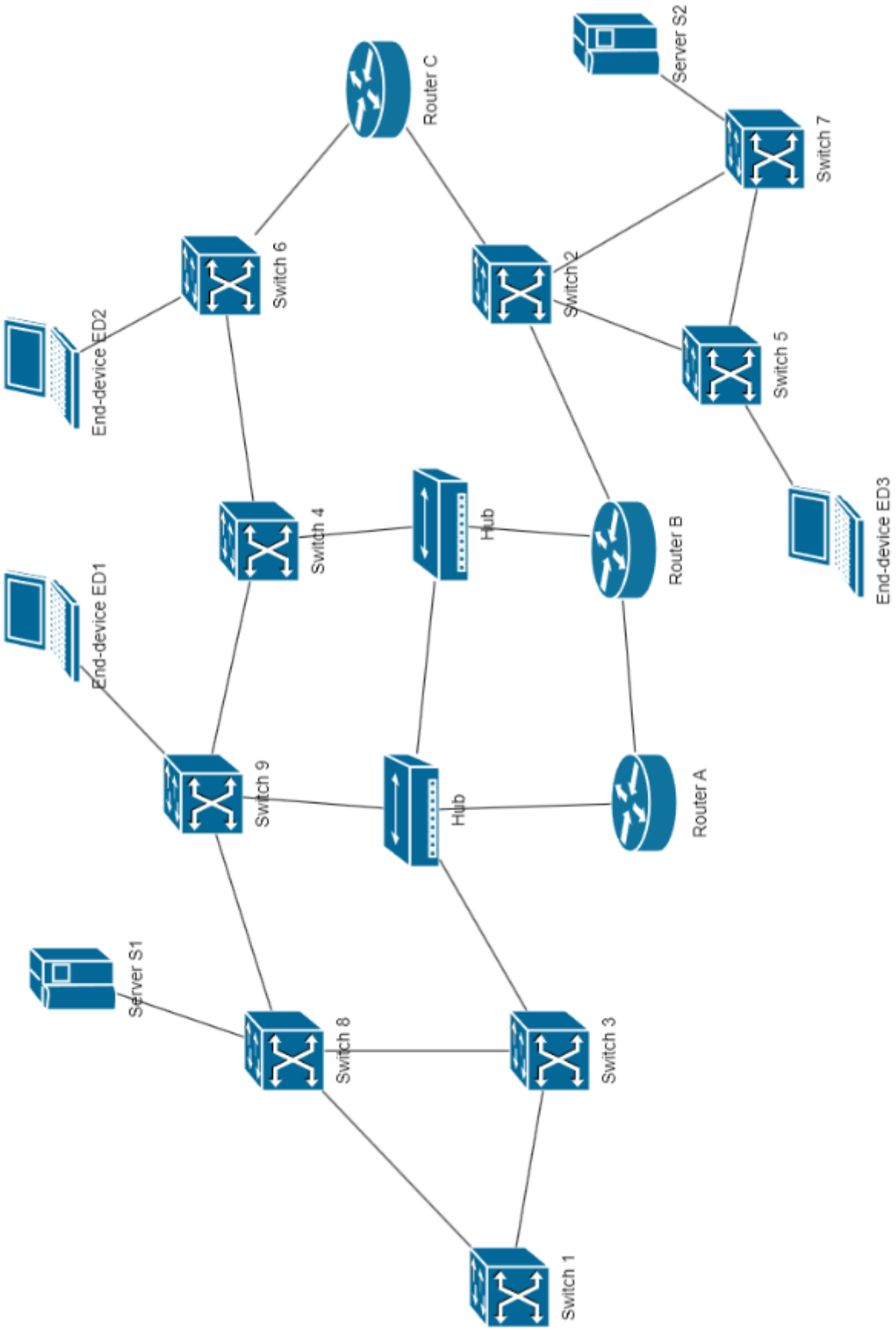

Figure 1. Un réseau d'entreprise.

Question 3.2 (3 points) : << Password manager LastPass disclosed a breach in August 2022. That disclosure revealed that an intruder had access to archive data held on a third-party cloud region. Later in a blog from the CEO Karim Toubba, it was also admitted that data obtained from the initial attack was used to compromise another employee. Credentials and keys were stolen, enabling access to encrypted data on the third-party cloud region. While LastPass are at pains to stress that the security of a customer's password data is dependent on their master password, which LastPass does not have access to, it remains the case that with access to a customer's encrypted passwords themselves, an attacker could attempt to brute force them. This would depend on the strength of the master password selected by the user. Unfortunately, history and experience tell us that many master passwords are likely to be sub-optimal and liable to attack. >>

- Dans une application de type « gestionnaire de mots de passe » comme LastPass, est-il vrai que la sécurité des mots de passe d'un client dépend de la sécurité du mot de passe principal du client ? Est-il vrai que LastPass ne dispose pas du mot de passe du client ?
- Expliquez la phrase « with access to a customer's encrypted passwords themselves, an attacker could attempt to brute force them », en détaillant comment l'attaquant opère.
- Expliquez la phrase « history and experience tell us that many master passwords are likely to be sub-optimal and liable to attack ».

Question 3.3 (4 points) : << Caesars Entertainment, the self-proclaimed 'largest U.S. casino chain with the most extensive loyalty program in the industry' had its database of loyalty customers stolen. The problem was noticed on September 7th and Caesars immediately filed form 8-K with the US Securities and Exchange Commission to report the attack. Caesars also stated, 'We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor.' It also appears that Caesars paid a ransom of around $15 million to avoid publication of the stolen data. The ransomware gang had originally asked for $30 million. Bloomberg later reported that the breach was by Scattered Spider, a cybercrime group also known as Roasted 0ktapus and UNC3944. Caesars later published more details describing that the breach occurred through social engineering on an outsourced vendor used by the company. Having paid the ransom, Caesars cannot guarantee to their loyalty customers that their data is not at risk and are now scanning darknet sites, promising to alert customers if their data is discovered and offering complimentary giveaways and free services to customers to protect their data in the future. >>

- Détaillez l'attaque d'après les éléments fournis dans cet extrait.
- Détaillez et commentez cette phrase : « We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor ».
- Détaillez et commentez cette phrase : « Having paid the ransom, Caesars cannot guarantee to their loyalty customers that their data is not at risk ».
- Détaillez et commentez la réponse de l'entreprise.