**SISR(suite 1ère feuille) :**

service email :

- gmail
- outlook
- yahoo

Protocol :

- smtp → envoie de mails, port=25
- pop → réception de mails, port=110
- imap → réception de mails, port=143
- https → trafic web sécurisé et données chiffrées, port=443
- http → trafic web non sécurisé, port=80
- ftp → transfert de fichiers, port=21
- ldap
- dns → résolution de noms, port=53
- icmp → Ping (tester la présence), port=7

Exemples en bas

protocol pop, les mails ne seront pas actualisé comme lu sur tous nos appareils car ne va pas les actualiser comme lu car synchronisation unidirectionnel (télécharge juste les mails du serveur à notre pc)
alors que le imap lui effectue une synchronisation dans les deux sens

Technologie :

- Exchanges

(rechercher liens entre les 3)

Installation → sécurisation → amélioration (installation d'équipements ou de logiciels en entreprise)

Protocole → port de communication entre deux équipements actifs compatibles
→ compréhension commune du protocole

dif éléments actifs et passifs :

éléments actifs → émission, réception + traitement (PC, imprimantes, routeurs)
éléments passifs → émission, réception (switch, hub, transceiver)

éléments actifs vont interagir avec le collaborateur alors que les passifs vont interconnectés les équipements

Modèle OSI :
(regarder fonctionnement)

1) Physique
2) Liaison de données
3) Réseau
4) Transport
5) Session
6) Présentation
7) Application

de 1 à 4 = passifs et donc de 5 à 7 = actifs

Exemples protocol :
→ consulter une page internet 80 – 443 – 53
→ consulter email outlook 143 ou 110 – 53 et 25 si accusé de réception est envoyé lors de l'ouverture d'un mail
→ envoyer des infos sur un serveur web 21 – 53
→ réveiller un équipement 7 – 53
→ acheter un ordi sur internet 443 – 53

Le DNS est présent de partt

Interconnexion PC-serveur (câbles de connexion) :

RJ45 = classique → performances → 1gb/s (longueur max câble = 100m, mais on peut parcourir des longues distances en intercoupant avec des switchs à moins de 100m de distance chaque fois et bien sur il faut des bâtiments ou intermédiaire qui nous appartiennent)
Fibre = coûteux++ → performances → illimité
Wifi = performances → 300mb/s

boîtier pour passer de fibre à RJ45 = transceiver (éléments passif car ne traite pas le signal, le retransmet juste)

TP :

commande pour terminal :

ping+IP(pour ping) en entreprise le temps max doit être 1ms et il diffère selon si la connexion est par câble ou wifi et sont bloqués si pare-feu activé
ping -a + IP(pour avoir nom IP)
tracert + IP(pour savoir combien de router traversés)

si au sein du même réseau un ordi est plus lent qu'un autre on ping la passerelle avec

les deux.
Selon le temps de réponse le pb peut venir du port du switch ou du câble, du hub(normal car duplique les paquets sur tt les ports)

telnet = port 23
Pour voir un port → nom du port + nom du site (pas sur chercher et aussi comment les ouvrir et les fermer)

une authentification ne veut pas dire que les données sont chiffrées

si pas le « s » de chiffré dans le protocol nos données seront en clair et notre mdp sera donc visible

Stratégie pour un client :

- utiliser les protocol SFTP (protocol ftp chiffré) et HTTPS
- fermer certains ports
- faire des sauvegardes (système ou site internet …)

les alertes de sécurité passe de 20% à 95% la veille des jours fériées

Qlq types de cyber attaques → Ranbonware, Fishing, cheval de troie