**Le système d’Exploitation**

**Formatrice : Florence CALMETTES**

**Durée totale du module : 14 heures**

**Travail à Effectuer 2 : Compréhension du rôle du Système d’Exploitation :**

**Remplir le tableau suivant :**

|  |  |
| --- | --- |
| **Consigne** | **Réponse** |
| Quels sont les étapes de démarrage de l’ordinateur ? | • BIOS (ou Séquence-POST) = Analyse les composants physiques, identifie les périphériques puis analyse l’ordre de priorités.  • MBR et Boot = contient la table des partitions du disque dur et un chemin logique d’amorçage pour le système d’exploitation, puis le Boot est la procédure de démarrage du système d’exploitation.  • NTLDR = charge la partition active (étape du choix de l'os si multi-boot)  • NTOSKRNL.exe = Log ON Choix et démarrage de la session.  • Bips et Alertes = Alarme venant de la carte mère, blue screen, etc… |
| Qu’est-ce que la communication Homme / Machine ? | C’est la comunication entre l’utilisateur et l’odrinateur (à double sens) via une interface graphique ou des comande (MS-Dos, Linux,…)  Cette communication permet à l’utilsateur l’execution d’actions (tâches)(modifié) |
| Citez des périphériques d’entrée ? | Claviers, souris, micro, scanner, pad tactile, manette de jeu, etc. |
| Citez des périphériques de sortie ? | Casque, écran, enceinte, imprimante, etc. |
| Citez des périphériques d’entrée et de sortie ? | Clef USB, HDD, câble réseau et carte réseau, etc. |
| Qu’est-ce que l’IRQ ? Comment fonctionne l’IRQ ? | L’IRQ est l’interruption matérielle.  La table IRQ hiérarchise les périphériques (le clavier est par exemple le numéro 1). Il détermine quand une action physique se lance et se termine. Permet aussi d’interrompre une action en cours.(modifié) |
| Qu’est-ce qu’un processus ? | C’est une tâche ou application en cours d’exécution. |
| Qu’est-ce que l’ordonnanceur ? | Une « inscription » en dur rattaché au CPU.  Fonction Interne au pross. qui contrôle et pilote l'exécution des autres programmes tournant sur la machine et leur ordre de priorité. |
| Quel rôle joue le système d’exploitation dans la gestion des fichiers ? | Il en a deux :   1. Gestion de la mémoire permanente (mémoire morte)   Organisation par arborescence du disque dur.   1. Système de gestion de fichiers (format)   Les plus connu / courrants sont le Fat32 et NTFS sur windows, ExT4 pour Linux. Attention, NTFS ne marche pas sous Mac (spécialité dev par windows) |
| Définir API ? | Interface qui sert de façade pour gérer les ports et les protocoles pour les logiciels. (Chaque service à un ou plusieurs protocoles et chaque protocole a son propre port dédié) |

**Travail à Effectuer 3 : Installation du poste de travail :**

Definir NTFS et FAT

FAT : système de fichiers utilisable sur la plus part des OS mais peu sécurisé et n’offrant que peu d’options, la taille des fichiers y est limité à 4go et celle des partitions à 2To

NTFS : Système de fichiers Windows permettant une plus grande sécurité, notamment en local, l’utilisation de quotas d’utilisation, la journalisation et d’enregistrer des fichiers de grande taille.

**Travail à Effectuer 4 : Configuration du Système MsConfig :**

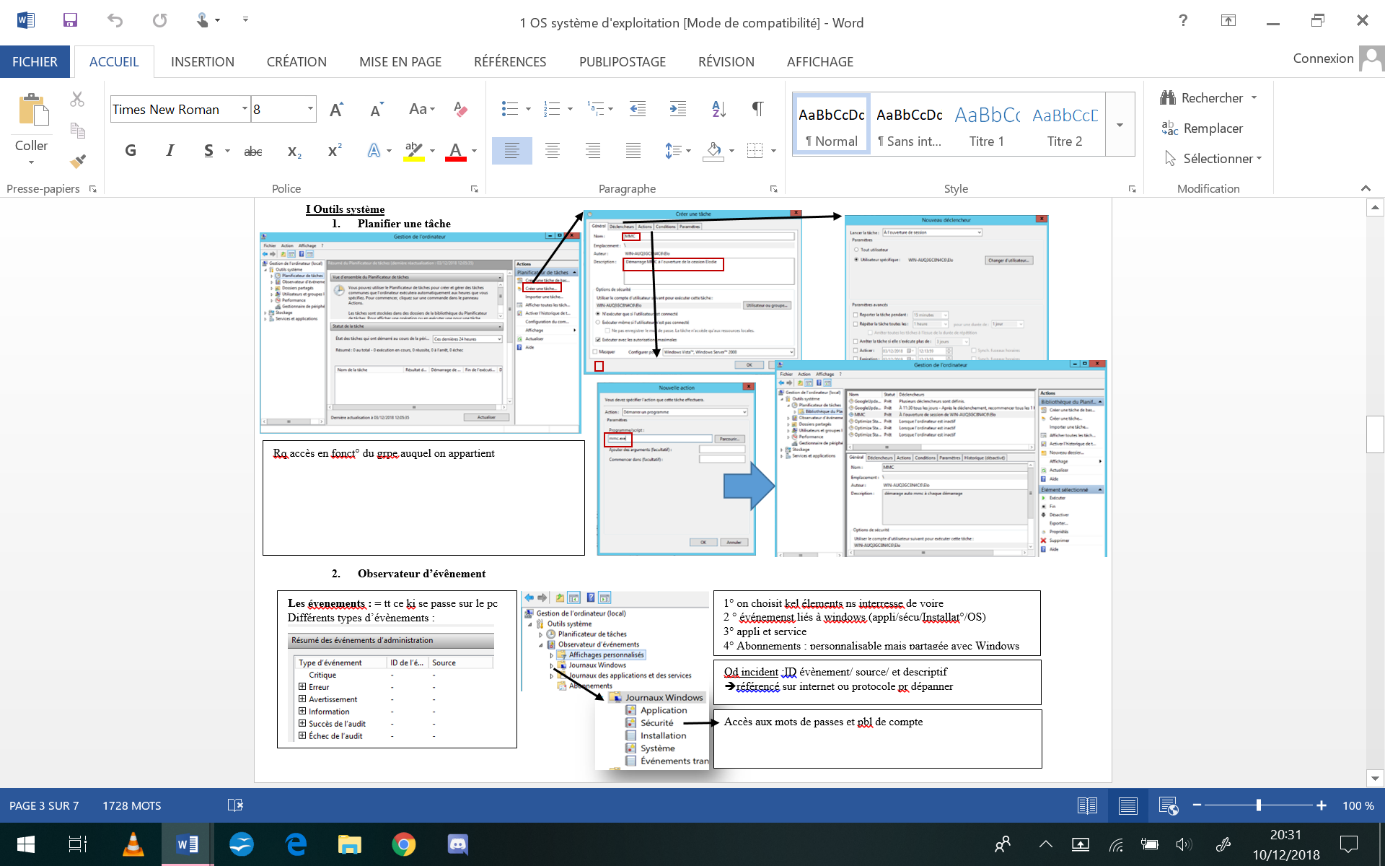
**Remplir le tableau suivant :**

|  |  |
| --- | --- |
| **Consigne** | **Réponse** |
| Que veut dire Démarrage Normal ? | Démarrage classique / standard |
| Que veut dire Démarrage En mode Diagnostic ? | C’est un démarrage permettant de charger seulement les pilotes de périphérique et les services de base équivalent au mode sans échec(modifié) |
| Que veut dire Démarrage Sélectif ? | Le démarrage sélectif permet de personnaliser le démarrage en fonction de nos besoins (Charger les services système, charger les éléments de démarrage, utiliser la configuration de démarrage d’origine). |
| Qu’est-ce qu’un démarrage sécurisé – minimal ? | Le démarrage minimal, sans réseau, avec simplement les pilotes (et services) de base. Globalement, l’ancien « démarrage sans échec sans prise en charge réseau ». |
| Qu’est-ce qu’un démarrage sécurisé – Autre environnement ? | Il permet de garder le démarrage minimal mais sans la prise en charge de l’interface graphique. |
| Qu’est-ce qu’un démarrage sécurisé – Réseau ? | Mode sans échec avec réseau |
| Que veut dire GUI ? | Graphical User Interface - Interface graphique utilisateur |
| A quoi sert l’onglet Services ? | L’onglet Services (API) permet de visualiser, activer ou désactiver au démarage un ou des services disponibles de Windows |

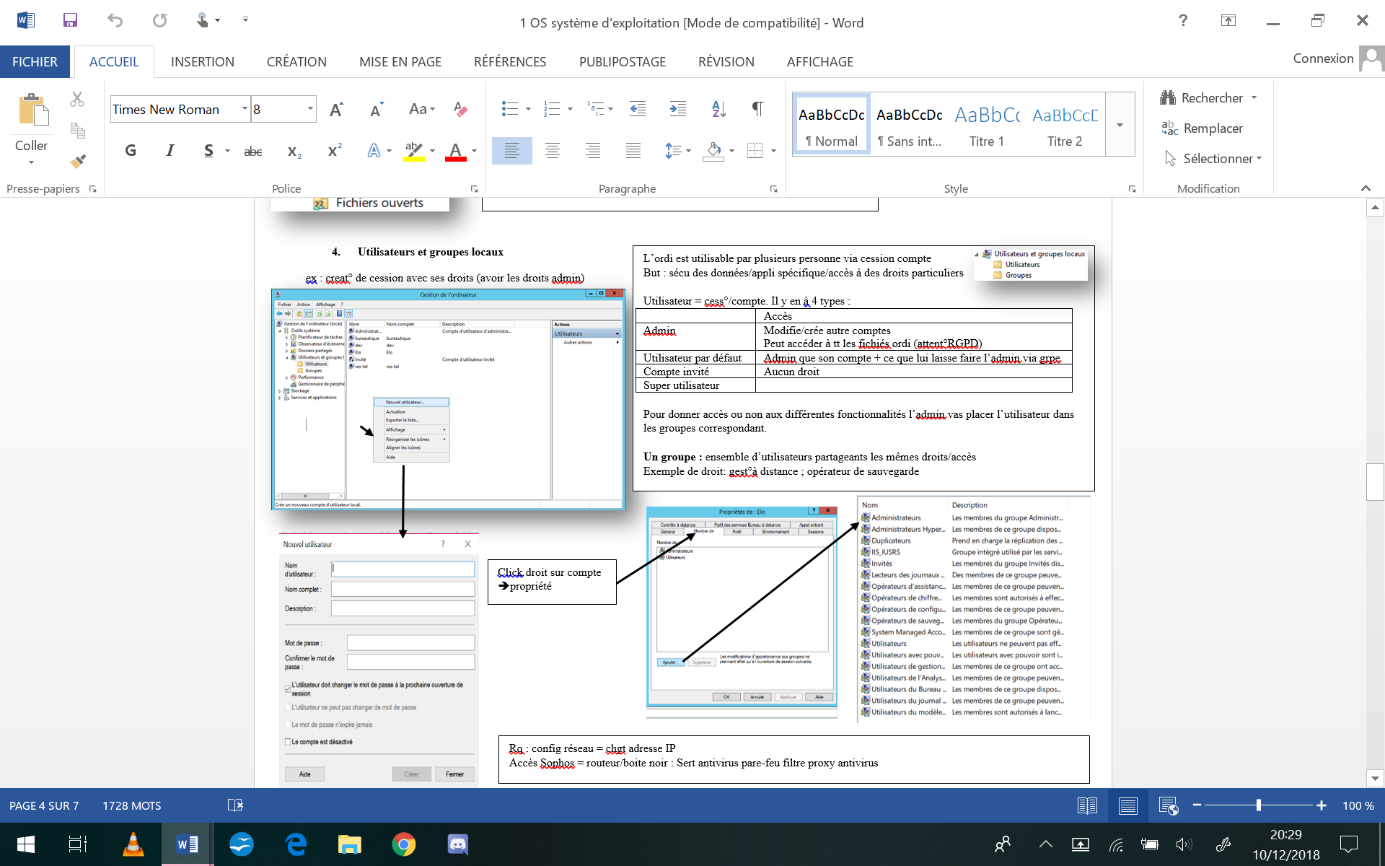
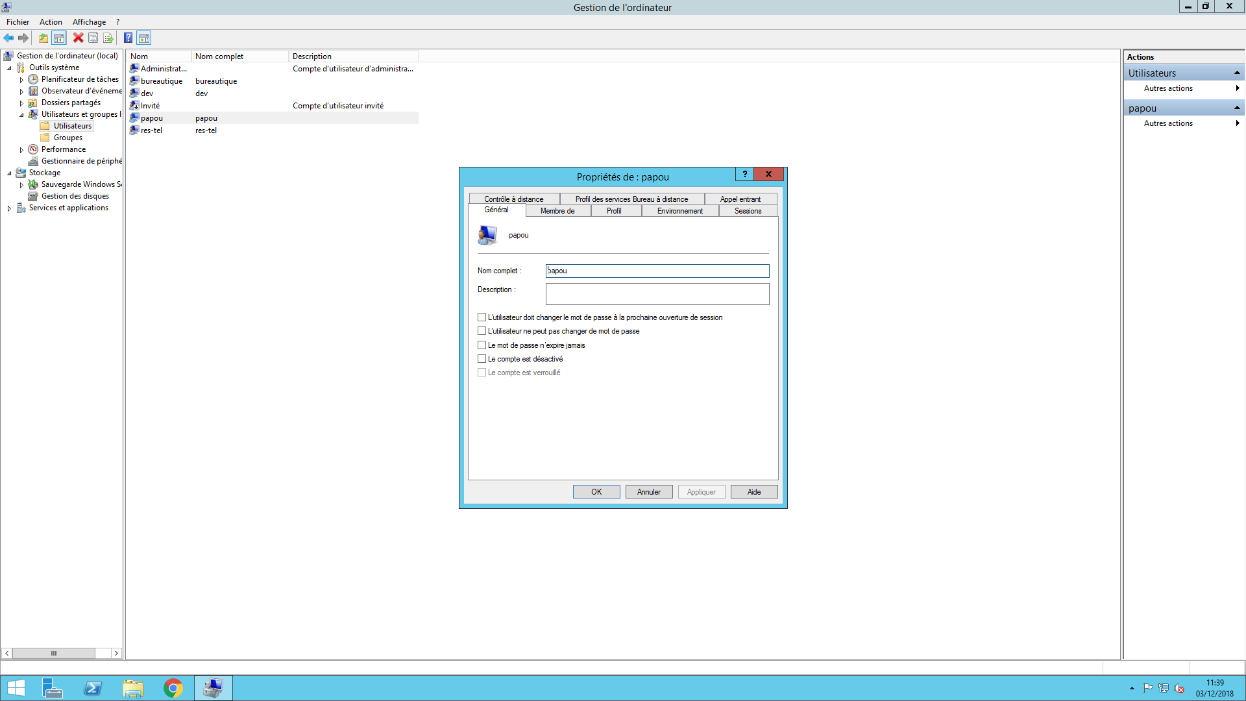
**Travail à Effectuer 5 : Gestion de l’ordinateur :**

**Pour chacune des consignes ci-dessous, merci de faire une capture d’écran**

- Création d’une tâche planifiée qui démarrer la console MMC



- Création d’une session utilisateur avec droit admin + session Papou



|  |  |
| --- | --- |
| **Consigne** | **Réponse** |
| Quels sont les différents types d’évènement ? | Critique, erreur, Avertissement, Information, Succès ou Echec de l’audit (Débogueur de problèmes liés à la sécurité). |
| Dans l’observateur d’évènement en cas d’erreur, quel est la procédure à adopter ? | Avant tout vérifier trois choses :  - Quel est l’ID de l’évènement (référence potentielle sur le net)  - La source de l’évènement.  - Le descriptif de l’évènement (plus de détail concernant la cause) |
| Quels sont les différents dossiers dans l’observateur d’évènement et leur rôle ? | * Affichage personalisé : permet de créer une vue personalisée sur différents évènements selectionnés. * Journaux windows : répertorie l’historique des installations, alertes de sécurités, erreurs, tous les évènements du système. * Journaux des applications et des services : Il recense tous les évènements qui se sont produits sur la machine en les organisant par dossier. * Abonnements : permet de créer des abonnements pour visualiser les évènement d’autres PC du réseau. |
| Qu’est-ce qu’un utilisateur ? | L’utilisateur est soit :   * Le compte de session standard bénéficiant des droits communs, enregistré, faire des mises à jour, etc. Aucun droit admin, mais bien plus de droits que l’invité.   Soit   * L’appellation globale de la personne qui utilise le pc, par défaut l’utilisateur principale de ce dernier.   L’utilisateur fait généralement parti du groupe utilisateur s’il est sur un appareil commun est à sa propre session. |
| Qu’est-ce qu’un groupe ? | Un groupe est un ensemble d’utilisateurs auxquels on attribue des autorisations, des interdictions… Il détermine les droits d'accès selon une certaine hiérarchie. |
| Qu’est-ce qu’une partition principale ? | Partition de la table de partitions principale dans laquelle il est possible de créer un maximum de 4 partitions, principales ou étendues. C’est le seul type de partition permettant l’installation des systèmes d’exploitation Windows |
| Qu’est-ce qu’une partition étendue ? | Une partition étendue ressemble à une partition principale si ce n’est qu’elle est capable de recevoir autant de partitions qu’il ne reste de place (elles sont alors appelées partitions logiques) |
| Qu’est-ce qu’une partition active ? | Une ***partition active*** est une partition sur laquelle on retrouve le système d’exploitation.  Ne pas confondre avec :  On doit rendre une partition *active* pour qu’elle soit prête à être formatée (en ntfs ou fat32) |
| Qu’est-ce qu’un service ? | Un processus du système tournant en permanence en tache de fond et contrôlant ports & protocoles pour les applications, aussi appelé API |
| Quels sont les types de démarrage d’un service ? | Automatique, Automatique différé (avec un temps défini avant son lancement après le démarrage), Manuel ou Désactivé |
| Quels sont les différents états d’un service ? | En cours, arrêté, suspendu. |
| Comment changer l’état d’un service ? | Propriété sur le service concerné / puis sélectionner l’état que l’on souhaite dans la liste. |

**Travail à Effectuer  6 : Base de Registre :**

|  |  |  |
| --- | --- | --- |
| **Consigne** | **Arborescence dans la base de registre** | **Clé modifiée et Valeur** |
| Afficher un message à l’ouverture de session | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon | LegalNoticeCaption :  message de bienvenu  LegalNoticeText :  message d'accueil |
| Activer la touche NUMLOCK au démarrage | HKEY\_CURRENT\_USER\Control Panel\Keyboard  HKEY\_USERS\.DEFAULT\Control Panel\Keyboard | InitialKeyboardIndicators 2 = activé / 0 = éteint  InitialKeyboardIndicators  2 = activé / 0 = éteint |
| Supprimer l’icône volume dans la barre des tâches | HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer | Nouvelle clé « Explorer », nouvelle valeur REGDWORD  HideSCAVolume  = 1 |
| Désactiver l’usb (sur VM ) | HKEY\_LOCAL\_MACHINE, System, CurrentControlSet, Services, UBSTOR | Start = 4 |
| Désactiver le cmd ( sur VM ) | HKEY\_CURRENT\_USER, Software, Policies, Microsoft, Windows, System | DisableCMD = 1 |

**Travail à Effectuer 7 : Configuration de la console MMC :**

Créer des raccourcis vers les fonctionnalités vues précédemment.

Faire une capture d’écran.

