

TP DE FIN DE MODULE

Fondamentaux TIP

Mise en service et diagnostic d'un poste informatique

Durée indicative : 1 h 30 à 2 h | Niveau : Débutant | Module : Fondamentaux TIP

Objectif du TP

Mobiliser les acquis du module 0 : matériel, stockage, Windows, comptes, CMD/PowerShell, virtualisation, réseau et cybersécurité. L'objectif est de vérifier un poste, diagnostiquer une anomalie simple et documenter l'intervention.

Contexte

Tu travailles au sein d'un service informatique. Un poste doit être préparé pour un nouvel utilisateur. Avant sa remise, ton responsable te demande de vérifier son état matériel, système, réseau et sécurité, puis de rédiger un compte rendu synthétique.

Avant de commencer

- Utiliser un poste ou une VM de laboratoire ne contenant aucune donnée importante.
- Créer un snapshot si le TP est réalisé dans une machine virtuelle.
- Préparer une fiche d'intervention pour noter les résultats.
- Observer avant de modifier : ne changer une configuration que si cela répond à un problème identifié.

Compétences mobilisées

- Identifier les caractéristiques d'un poste.
- Contrôler le stockage et les partitions.
- Vérifier Windows et les périphériques.
- Identifier les comptes et privilèges.
- Utiliser CMD et PowerShell.
- Contrôler IP, DHCP, DNS et connectivité.
- Vérifier mises à jour, antivirus et pare-feu.
- Reconnaître une situation de phishing et adopter les bons réflexes.

Mission 1 - Identifier le poste

Utilise hostname, whoami, msinfo32 ou systeminfo. Relève les informations suivantes :

Nom du poste	
Utilisateur	
Version de Windows	
Processeur	
Mémoire RAM	
Architecture	

Mission 2 - Contrôler le stockage

Ouvre diskmgmt.msc ou utilise Get-Disk, Get-Partition et Get-Volume. Observe les disques, partitions, volumes, lettres et systèmes de fichiers.

Combien de disques physiques sont présents ?

Quel système de fichiers est utilisé par le volume Windows ?

Quelle est la différence entre un disque physique et une partition ?

Quel est le rôle de la partition EFI sur un système UEFI ?

Mission 3 - Contrôler Windows

Ouvre taskmgr et devmgmt.msc. Observe l'utilisation CPU/RAM/disque et recherche des périphériques inconnus, désactivés ou accompagnés d'un avertissement.

Réflexe technicien

Un point d'exclamation dans le Gestionnaire de périphériques peut indiquer un problème de pilote ou de fonctionnement matériel.

Mission 4 - Vérifier les comptes et les droits

Utilise whoami, whoami /groups, net user, ou PowerShell avec Get-LocalUser et Get-LocalGroupMember Administrateurs.

Quel utilisateur est connecté ?

Possède-t-il des droits administrateur ?

Pourquoi un utilisateur standard ne devrait-il généralement pas disposer de droits administrateur permanents ?

Mission 5 - Contrôler la configuration réseau

Exécute ipconfig /all et relève la configuration principale.

Adresse IPv4	
Masque	
Passerelle	
DNS	
DHCP activé	Oui / Non
Adresse MAC	

Réalise ensuite ces tests dans cet ordre :

- ping 127.0.0.1
- ping
- ping 8.8.8.8
- nslookup www.wikipedia.org
- Test-NetConnection www.wikipedia.org -Port 443

Méthode réseau

Interface -> IP -> passerelle -> IP distante -> DNS -> service. Avancer du plus simple au plus précis permet de localiser plus vite l'étape défailante.

Mission 6 - Utiliser CMD et PowerShell

Crée C:\Support, puis un fichier diagnostic.txt contenant le nom du poste, l'utilisateur et la configuration IP. Utilise les commandes vues dans TIP 0.9.

À quoi sert l'opérateur >> ?

Mission 7 - Vérifier la sécurité du poste

- Contrôler Windows Update.
- Vérifier Microsoft Defender et la protection en temps réel.
- Contrôler le pare-feu avec Get-NetFirewallProfile.
- Afficher les extensions de noms de fichiers.
- Vérifier qu'aucune alerte de sécurité inhabituelle n'est présente.

Pourquoi facture.pdf.exe doit-il attirer l'attention ?

Mission 8 - Diagnostiquer une panne réseau

Situation

Adresse IPv4 : 169.254.38.17

Masque : 255.255.0.0

Passerelle : aucune

L'utilisateur indique qu'il n'accède plus à Internet alors que ses collègues n'ont pas de problème.

Quel élément de cette configuration est anormal ?

Que signifie généralement une adresse 169.254.x.x sous Windows ?

Quel service faut-il vérifier en priorité ?

Quelles vérifications physiques ou réseau peux-tu effectuer ?

Quelles commandes permettent de demander une nouvelle configuration DHCP ?

Mission 9 - Situation de cybersécurité

Message reçu

URGENT - Votre compte sera désactivé.

Votre mot de passe expire dans 30 minutes. Cliquez immédiatement sur le lien suivant pour conserver votre accès.

Quels éléments doivent éveiller tes soupçons ?

Que dois-tu conseiller à l'utilisateur ?

Faut-il utiliser le lien contenu dans le message ?

Que faire si l'utilisateur indique avoir déjà saisi son mot de passe ?

Compte rendu d'intervention

Rédige un compte rendu professionnel et synthétique. Il doit permettre à un autre technicien de comprendre ce qui a été vérifié, l'anomalie éventuelle, les actions menées et le résultat obtenu.

Poste / utilisateur

Contexte de l'intervention

Contrôles réalisés

Anomalie(s) constatée(s)

Action(s) réalisée(s)

Résultat final

Méthode à retenir

Observer -> diagnostiquer -> agir -> vérifier -> documenter

Le résultat technique est important, mais la qualité d'une intervention repose aussi sur la méthode, la sécurité et la traçabilité.

Auto-évaluation

- Je sais identifier les caractéristiques principales d'un poste.
- Je sais distinguer disque, partition et volume.
- Je sais vérifier comptes et privilèges.
- Je sais utiliser CMD/PowerShell pour collecter des informations.
- Je sais contrôler une configuration IP et suivre une méthode de diagnostic réseau.
- Je sais vérifier les protections essentielles d'un poste.
- Je sais reconnaître plusieurs signes de phishing.
- Je sais rédiger un compte rendu d'intervention.