



le practical-work est pas trop claire pour moi : soit plus clair au niveau des dossiers que je dois y créer ? exemple tu m'a dis un dossier scans, mais scan de quoi ? puis script, script de quoi ? ect

Tu as raison de demander, on va le simplifier à fond et le lier à TON projet concret.

L'idée: 01-practical-work = tout ce que tu fais "en vrai" sur le réseau et le NAS.

Voici exactement les dossiers à garder et ce que tu mets dedans, avec des exemples très concrets.

1. 01-practical-work\scans

"Tout ce que tu scannes avec Nmap ou autre."

Tu mets ici UNIQUEMENT les fichiers de résultats de scans.

Exemples de fichiers que TU vas avoir:

- 01-network-discovery-2025-11-25.txt
 - résultat de: nmap -sn 192.168.1.0/24
- 02-router-scan-2025-11-25.txt
 - résultat de: nmap -sV IP_ROUTEUR
- 03-nas-main-fullscan-2025-11-27.txt
 - résultat de: nmap -sV -sC -p- IP_NAS_PRINCIPAL
- 04-nas-backup-fullscan-2025-11-27.txt
 - résultat de: nmap -sV -sC -p- IP_NAS_BACKUP

Donc: "scan de quoi ?" → scan du réseau, du routeur, du NAS principal, du NAS backup (avec Nmap).

À chaque fois que tu lances un nmap et que tu rediriges la sortie vers un fichier, tu le mets ici.

2. 01-practical-work\configs

"Comment le NAS et le réseau sont configurés."

Tu mets ici des fichiers texte qui décrivent la config, que tu notes toi-même à partir de DSM ou de ton PC.

Exemples:

- dsm-network-config.txt
 - IP du NAS, masque, gateway, DNS, ports DSM (5000/5001), etc.

- dsm-security-settings.txt
→ 2FA activé ou non, Auto Block, firewall DSM, politique de mot de passe, etc.
- dsm-shared-folders.txt
→ liste des dossiers partagés + droits (qui a accès)
- dsm-users-groups.txt
→ liste des comptes utilisateurs et groupes (sans mots de passe)
- backup-setup.txt
→ comment le backup est configuré (NAS principal → NAS backup, horaires, etc.)

Donc: "config de quoi ?" → config du NAS (DSM) et éventuellement de ton PC/routeur si utile.

3. 01-practical-work\logs

"Sorties brutes de commandes sur ton PC."

Tu mets ici ce qui sort de ton terminal (PowerShell), sans le modifier.

Exemples:

- ipconfig-2025-11-25.txt
→ résultat de la commande ipconfig
- route-print-2025-11-25.txt
→ résultat de route print
- arp-a-2025-11-25.txt
→ résultat de arp -a

Ce sont des "logs" de ton environnement, utiles pour l'analyse réseau.

4. 01-practical-work\outputs

"Résumés / fichiers où tu as déjà travaillé les résultats."

Tu mets ici les choses que tu as déjà un peu "nettoyées" ou organisées.

Exemples:

- scan-results.md
→ un fichier où tu as recopié les ports/services du NAS dans un tableau propre.
- nas-services-table.csv
→ un tableau (Excel/CSV) des services du NAS avec colonnes: port, protocole, service, version, remarque.
- risk-scores.xlsx
→ ton calcul de score de risques (impact × probabilité) si tu le fais dans Excel.

Donc: "outputs de quoi ?" → outputs de ton analyse à partir des scans et configs (les choses lisibles et prêtées à utiliser dans ton rapport).

5. 01-practical-work\screenshots

"Toutes les captures d'écran."

Tu mets ici les images que tu prends:

Exemples:

- day1\
 - dsm-dashboard.png
 - dsm-network-settings.png
 - dsm-shared-folders.png
- day2\
 - nmap-fullscan-nas-main.png
 - dsm-security-settings.png

Tu peux faire un sous-dossier par jour ou par thème, comme tu préfères.

Ces images te serviront pour ton rapport et pour prouver que tu as vraiment fait le travail.

6. 01-practical-work\scripts

"Petits scripts pour t'aider (OPTIONNEL mais très bien vu)."

Tu n'es pas obligée d'en faire, mais vu ton niveau, c'est un plus.

Exemples possibles:

- run-nas-scans.ps1
 - script PowerShell qui lance automatiquement plusieurs commandes nmap sur le NAS.
- export-nmap-to-csv.py
 - petit script Python pour transformer un résultat texte en CSV.
- check-open-ports.ps1
 - script qui lit un fichier de scan et liste les ports ouverts.

Donc: "script de quoi ?" → script pour automatiser tes scans ou le traitement de résultats.

Si tu n'en fais pas, le dossier peut rester vide au début, ce n'est pas grave. Mais si tu as le temps, écrire 1–2 scripts simples, ça montre ton côté "ingénieur".

Pour simplifier au maximum

Si tu veux une version MINIMUM VIABLE, tu peux te concentrer sur:

- scans → tous les fichiers de résultats Nmap
- configs → tout ce que tu notes sur la config DSM
- screenshots → toutes les captures d'écran importantes
- outputs → 1 fichier scan-results.md avec tes tableaux propres

Et laisser:

- logs (si tu ne les utilises pas beaucoup)
- scripts (si tu ne fais pas encore de scripts)

Plus tard, quand tu seras plus à l'aise, tu rempliras logs et scripts.

Exemple concret avec CE QUE TU AS DÉJÀ FAIT

D'après ce que tu m'as dit, tu peux déjà ranger comme ça:

- 01-practical-work\scans
 - 01-network-discovery-2025-11-25.txt (nmap -sn 192.168.1.0/24)
 - 02-router-scan-2025-11-25.txt (nmap -sV 192.168.1.254)
- 01-practical-work\configs
 - dsm-network-config.txt (à créer: tu écris dedans IP du NAS, etc.)
- 01-practical-work\screenshots
 - day1\dsm-home.png (si tu as un screen de DSM)
 - day1\nmap-scan-router.png
- 01-practical-work\outputs
 - scan-results.md (à créer: tu résumes les ports trouvés sur le routeur et, plus tard, sur les NAS)

Si tu veux, tu peux me coller ici les noms EXACTS des fichiers que tu as déjà, et je te dirai:

- où les mettre,
- et éventuellement comment les renommer pour que ce soit clean et pro.