Plan de cours

Contient les plans de cours permettant la création du ruban pédagogique et l'organisation de l'année.

00 - Introduction à la formation (CIEL)

Durée approximative : ***1h***

Eléments du référentiel adressé : ***n/a***

I. Explication du contenu de la formation

- Gestion de projet
- Conception / validation / MCO d'une infrastructure IT industrielle
- Développement / BDD
- Cybersécurité
- Valorisation de la donnée

II. Présentation de l'examen

Présenter le contenu et les modalités de l'examen ainsi que ce qui est attendu sur les épreuves techniques

S'appuyer si nécessaire sur la documentation fournie dans le référentiel.

Evaluation : Procéder au test de positionnement.

> **Tu me dis, j'oublie. Tu m'enseigne, je me souviens. Tu m'implique, j'apprends.**

> - *Benjamin Franklin*

III. Note aux formateurs

Pour la suite du plan de cour, les cours seront découpés en modules appartenant tous à un Thème.

Les thèmes sont définis comme suit :

1. Infrastructure & Systèmes
2. Réseaux (informatique et industriel)
3. Développement (code, scripts, automatisation)
4. Gestion de projet
5. Cybersécurité et valorisation de la donnée

Les modules seront ensuite numéroté en fonction de l'ordre dans lequel les aborder.

Chaque module aura en en-tête les points du référentiel adressés et la durée approximative du module.

Ressources associées :

n/a

1.01 - Introduction Générale à l'informatique

Durée approximative : ***2h***

Eléments du référentiel adressé :

- ***U4 - étude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R5 : Maintenance des réseaux informatiques***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***

I. Qu'est-ce q'un ordinateur

Définition de l'ordinateur. S'appuyer sur EXT - wikipedia : ordinateur

Quelles sont ses formes (*desktop, laptop, mini-pc, barebone, raspberry pi, thin clients, tablettes, ...*).

> **Co-enseignement** : Il pourra être intéressant de se coordonner avec le professeur de Français pour avoir un cour sur l'histoire de l'informatique.

> **Conseil** : il peut être utile à ce stade de disposer de plusieurs matériels pour illustrer le propos et le leur faire manipuler.

II. Les différents composants

- **Alimentation**
  - Principaux fabriquants (*corsair, msi, ...*)
  - Type (*modulaire, non modulaire, formats, ...*)
  - Caractéristiques techniques notables (puissance, certification, connectique présente*)*
- **Carte mère**
  - Caractéristiques techniques notables (*socket, ports présents, quantité de RAM prise en charge, chipset constructeur*)
- **CPU**
  - Principaux fabricants (*intel, amd, qualcomm, ...*)
  - Architectures (*x86, x64, xeon, arm, ...*)
  - Caractéristiques techniques notables (*socket, cores, hyperthreading, fréquence, performancecore vs efficiencycore, ...*)
- **Carte graphique**
  - Principaux fabricants (*intel, nvidia, amd, ...*)
  - Caractéristiques techniques notables (*fréquence, vitesse de traitement, SLI, ...*)
- **Stockage**
  - Types de stockages (*HDD, ssd, flash, ...*)
  - Principaux fabricants (*western digital, corsair, ...*)
  - Caractéristiques techniques notables (*type de mémoire, capacité, connectique, vitesse lecture/ecriture, durabilité, ...*)
- **Connectivité réseau**
  - Cartes intégrées et cartes d'extension

> **TP** : ouvrir un PC, faire identifier les composants, ouvrir un serveur, faire de même et pointer la redondance matérielle. Noter également que la plupart des composants sont enfichables.

> **TP** : faire analyser une ou plusieurs fiches matérielles et demander à quel usage cela correspondrait. Puis indiquer un usage et demander les spécifications matérielles nécessaires.

III. Le système d'exploitation

Listing de version et historique des systèmes windows.

Listing de version et historique des systèmes linux.

- Principes de l'opensource
- s'appuyer sur EXT - Wikipedia : Linux
  - notamment pour illustrer les principes des distributions et de variantes.

IV. Le modèle client / Serveur

Définir les principes de l'architecture client/serveur et son fonctionnement.

Parler des spécificités OS pour chaque rôle et de ce qui les différencie.

Ressources associées :

Général - Un ordinateur

1.02 - Installation des systèmes

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées et réparties.***
      - ***Méthodologie de recherche et d'analyse de documentation y compris en anglais***
    - ***C05 : Concevoir un système informatique***
      - ***Infrastructures logicielles : centralisées, décentralisées ou réparties***
    - ***C09 : Installer un réseau informatique***
      - ***Systèmes d'exploitations (Window, Unix, virtualisation)***
    - ***C10 : Exploiter un réseau informatique***
      - ***Outils de mise à jour système et de sécurité système***
      - ***infrastructures matérielles***
      - ***infrastructures logicielles : centralisées, décentralisées et réparties***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R3 : Exploitation et maintient en condition opérationnelle***
    - ***C09 : Installer un réseau informatique***
      - ***Systèmes d'exploitations (Window, Unix, virtualisation)***
    - ***C10 : Exploiter un réseau informatique***
      - ***Outils de mise à jour système et de sécurité système***
      - ***infrastructures matérielles***
      - ***infrastructures logicielles : centralisées, décentralisées et réparties***

I. Préparation des Postes et espaces de travails

Téléchargement des sources sur les sites officiel (recherche assistée des sources et de la documentation associée).

Préparation des média d'installation avec rufus (recherche assistée des sources et de la documentation associée).

Accès au bios et présentation de celui-ci (recherche de documentation constructeur).

Installation des Systèmes (Windows 11 si possible).

> **Conseil** : Profiter des temps morts de l'installation pour échanger et consolider les acquis.

Recherche de packages de drivers et updates via le site constructeur.

> **Point sécu** : Expliquer l'impératif de maintenir ses systèmes à jour, pour avoir les derniers correctifs de sécurité.

> **Conseil** : Si c'est un PC portable, faire activer bitlocker et sécuriser la clé de récupération. Expliquer l'intérêt de BitLocker. Parler du risque de vol de matériel et de la démo technique du hack de la surface pro.

Installation d'un environnement linux sur WSL.

Installation d'un logiciel manuellement (suite office par exemple).

Installation de l'environnement de travail et des logiciels à travers un script winget.

> **Conseil** : utiliser les temps morts de l'installation pour échanger sur les sujets abordés afin de consolider les acquis.

Ressources associées :

Rufus - Création d'un média d'installation

Windows11 - Installation

Windows11 - Installer linux avec WSL

1.03 - Connaître ses systèmes

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C09 - Installer un réseau informatique***
      - ***Systèmes d'exploitation (Windows, Unix, virtualisation)***
    - ***C10 - Exploiter un réseau informatique***
      - ***Interface ligne de commande d'équipements et de systèmes d'exploitation***
    - ***C11 - Maintenir un réseau informatique***
      - ***Outillage nécessaire au diagnostic, à la réparation et les équipements de rechange***
- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R3 : Exploitation et maintien en condition opérationnelle***
    - ***C09 - Installer un réseau informatique***
      - ***Systèmes d'exploitation (Windows, Unix, virtualisation)***
    - ***C10 - Exploiter un réseau informatique***
      - ***Interface ligne de commande d'équipements et de systèmes d'exploitation***
    - ***C11 - Maintenir un réseau informatique***
      - ***Outillage nécessaire au diagnostic, à la réparation et les équipements de rechange***

> **Conseil** : Ce cour sera séparé en deux cours distinct. Un pour windows et un pour linux. Mais ils suivront le même plan.

I. La structure des systèmes de fichier

Comment est structuré le système de fichier. Qu'est-ce qui se trouve dans les dossier et quelle en est l'utilité.

- La spécificité de windows concernant le registre.
- La spécificité linux du 'tout fichier'

II. Les différents systèmes de fichier

Le partitionnement des disques, les types de disques, les types de partition, le secteur de boot.

Explication (sans renter dans du trop technique) des différents systèmes de fichiers et leurs limitation (FAT, NTFS, ext4, ...).

Explication LVM et partitions logiques.

III. Les utilisateurs et groupes locaux

Les Utilisateurs, Les groupes et la gestion de droits.

Gestion des droits côté NFS, côté POSIX.

Les fichiers importants sur linux (/etc/passwd, /etc/groups)

La notion de sudo.

IV. Les principales commandes systèmes

Apprentissage et utilisations des différentes commandes systèmes de bases.

> **Conseil** : Mettre à disposition des index contenant les commandes principales et leur utilité.

V.Gestion des services et processus

Expliquer les notions de services et processus ainsi que ce qui les différencie du windows au linux.

Montrer et apprendre comment les gérer (démarrage, arrêt, authentification,...)

VI.Gestion des Tâches planifiées et des cron

Expliquer comment gérer l'exécution des tâches planifiées.

Les différences en windows et linux avec les CRON.

Montrer et apprendre à créer, gérer les tâches planifiées.

Ressources associées :

Ubuntu - système de fichier

Ubuntu - Commandes utiles

Ubuntu - Gestion des droits

1.04 - Composantes de l'infrastructure informatique

Durée approximative : ***2h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R5 : Maintenance des réseaux informatiques***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***

I. Composantes de l'infrastructure

S'appuyer sur le schéma d'architecture d'une infrastructure informatique pour expliquer les différentes briques de l'architecture des systèmes d'information et l'interdépendance entre elles.

II. Les hyperviseurs

Définir la notion d'hyperviseur (Du serveur à la VM et au container).

La nécessité et les avantages de décorréler le matériel et les systèmes.

Les types d'hyperviseurs et leurs différences dans le fonctionnement et l'architecture.

Les principaux acteurs du marché et leur comparaison (licencing, performance, philosophie, cible de marché)

III. Les équipements de stockage

> **Conseil** : il peut être utile à ce stade de disposer de plusieurs matériels pour illustrer le propos.

Le NAS/ Le SAN et les baies de stockage.

La nécessité et avantages de décorréler le stockage et le système ou le compute

Les systèmes de sécurité et de redondance matérielle (RAID)

Parler également des différents protocoles réseaux de communication avec le stockage (ISCSI, fc, ...)

IV. Les équipements réseau (infrastructure)

Présenter les différents équipements réseaux et expliquer leurs rôles.

> **Conseil** : il peut être utile à ce stade de disposer de plusieurs matériels pour illustrer le propos.

- **Le switch**
  - switch vs hub
  - Rôle du switch
  - Principaux constructeurs (*HPE, aruba, cisco, dlink, ...*)
  - Caractéristiques techniques (*Nb de ports, capacité du fond de panier, connectique, firmware, stackable, ...*)

    - Note : les notions L2, L3 seront abordés dans le cours sur le modèle OSI
- **Le routeur**
    - Rôle du routeur
    - Principaux constructeurs (*Cisco, d-link, ...*)
    - Caractéristiques techniques (*Nb ports, débit max, possibilité de redondances, ...*)
- **Le pare-feu**
    - Rôle du pare-feu
    - Principaux fournisseurs (*Cisco, OPNsense, Sophos, Fortinet, Stormshield, ...*)
    - Caractéristiques techniques (*Nb ports, débit max, redondance, fonctionnalités présentes, IDS/IPS, ...*)
- **Les équipements wifi**
    - Rôle des bornes wifi, répéteurs et contrôleurs.
    - Principaux fournisseurs (*Cisco, HPE, D-link, ...*)
    - Caractéristiques techniques (*Débit, norme wifi B/G/N, portée, ...*)

Evoquer les autres équipent connectés comme les imprimantes, terminaux spécifiques

Evoquer les smartphones.

> **Co-enseignement** : Les spécificité des connectiques comme le support cuivre et fibre optique se feront par le prof de physique.

IV. Les équipements réseau (VoIP et industriels IoT)

Présenter la téléphonie sur IP, les téléphones et les équipements d'infrastructure (ipbx, SBC).

Présentation des équipement IoT, du concept de réseau industriel.

V. Le cloud

Définition des différentes solution cloud et des niveaux de service (iaas,paas,saas).

Ressources associées :

Méthodologie - Modèles d'architecture

Cloud : Niveaux de services

1.05 - Installer et manipuler l'hyperviseur

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***
    - ***C09 : Installer un réseau informatique***
      - ***Systèmes d'exploitations (windows, linux, virtualisation)***

I. Bases de la virtualisation

Rappel des bases évoquées plus tôt.

Point sur les types de virtualisation (bare metal, etc...)

Aborder les solutions bureautiques (hyper-v, vmware workstation, Virtualbox)

Aborder la "Nested virtualisation"

II. Installation et configuration

2.1 Installation de base

Installation et paramétrage de base de l'hyperviseur (heure/date, nom, réseau, domaine, updates, ...)

> **TP** : Faire installer un premier hyperviseur (vmware, hyper-V, proxmox).

Contexte : maintenant que son réseau est prêt, la société Labs404 à besoin d'installer un hyperviseur afin de virtualiser ses serveurs pour monter son infrastructure.

2.1 Configuration réseau et mise en place des SDN

Configurer les Vswitch et groupe de ports (paramétrer le SDN si disponible)

III. Mise en cluster

Afin d'assurer la haute disponibilité de l'infrastructure, procéder à la mise en cluster de l'hyperviseur.

Aborder les problématiques liées au stockage. Cela servira de passerelle au NAS, ISCSI et à la mise en place des baies de stockage.

Cela permet également d'aborder le concept de scalabilité.

> **TP** : Procéder à la mise en cluster du système de virtualisation et faire les réglages qui en découlent.

Contexte : Suite à une panne, la société Labs404 veut sécuriser son infrastructure pour assurer une continuité de service en cas de panne de l'un de ses hyperviseur.

Ressources associées :

Infrastructure - La virtualisation

1.06 - Configurer et sécuriser les accès distants

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C09 : Installer un réseau informatique***
      - ***Protocoles usuels SSH, RDP, WinRM***
      - ***Systèmes d'exploitations (Windows, UNIX)***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R3 : Exploitation et maintien en condition opérationnelle***
    - ***C10 : Exploirer un réseau informatique***
      - ***Interface en ligne de commande d'équipements et de système d'exploitation***
      - ***Connexion et prise en main à distance (protocoles et législation associée)***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D5 : Audit de l'installation ou du système***
  - ***C10 : Exploirer un réseau informatique***
    - ***Usage de documents règlementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

I. Introduction aux protocoles d'accès distants

Parler du principe d'accès distant.

Décrire le contexte législatif, notamment en ce qui concerne la prise en main à distance pour l'utilisateur (consentement, etc..)

Expliquer pourquoi il y a nécessité, à la fois pour des aspect réglementaire et de sécurité, d'utiliser des comptes nominatif et de loguer pour assurer une traçabilité des actions.

II. Le protocole SSH

Expliquer l'utilité et le fonctionnement du protocole SSH.

> **TP** : Faire installer le serveur ssh sur une VM linux et l'activer. Mettre un mot de passe faible et montrer un test de pénétration SSH.

Faire une analyse de risque. Faire chercher le guide des bonnes protiques de configuration SSH de l'anssi.

> **TP** : Reconfigurer le SSH en mode mot de passe et ajouter un compte automation avec authentification par clé.

Valider l'installation.

III. Le protocole RDP

Expliquer l'utilité et le fonctionnement du protocole RDP.

Montrer les failles du protocole. Parler du changement de méthode d'authentification (credssp) pour améliorer sa sécurité.

> **TP** : Faire configurer le RDP.

Faire une analyse de risque et chercher la documentation associée sur le site de l'anssi.

> **TP** : Appliquer les recommandations sur le paramétrage.

Valider l'installation.

IV. Le protocole winRM

Expliquer l'utilité et le fonctionnement du protocole winRM

Montrer les failles du protocole. Parler des listener et des trusted sources.

> **TP** : Faire configurer le winRM.

Faire une analyse de risque et chercher la documentation associée sur le site de l'anssi.

> **TP** : Appliquer les recommandations sur le paramétrage, désactiver le listener http et passer en https.

Valider l'installation.

V. Les autres protocoles

Evoquer les autres protocoles comme VNC, TeamViewer et rustdesk/anydesk (protocoles propriétaires)

Ressources associées :

<mettre ici les liens vers les pages ressources et support de cours>

2.01 - Principes des architectures réseau (CIEL)

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C06 : Valider un système informatique***
      - ***Modèle en couche***
    - ***C09 : Installer un réseau informatique***
      - ***Modèle en couche***
      - ***Protocoles usuel (IPv4, TCP/IP)***
- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R5 : Maintenance des réseaux informatiques***
    - ***C06 : Valider un système informatique***
      - ***Modèle en couche***
    - ***C09 : Installer un réseau informatique***
      - ***Modèle en couche***
      - ***Protocoles usuel (IPv4, TCP/IP)***

I. Le modèle OSI

Présentation du modèle OSI et de chaque couche. Mise à disposition si nécessaire du support de présentation.

Explications sur chaque couche. Sera vu ensuite tout au long des TP sur cisco packet tracer.

> **Conseil** : Le modèle OSI peut être vu au fil des TP. La couche 1 sera présentée avec du matériel. Le reste sera mis en pratique étape par étape sur cisco packet tracer.

> **Co-enseignement** : Les supports physiques de transmission (cuivre, fibre optique, etc...) seront vu avec le prof de physique.

Sur la couche 1, aborder les aspects sécurité avec les risques et les solutions (protection de l'accès à l'équipement, cache sur les ports)

II. Protocole IPv4

> **Co-enseignement** : Le binaire devra être maîtrisé avant cette étape. Cela sera géré par le professeur de mathématique.

Apprentissage des calcul d'adresses et de masques de sous réseau.

Voir les classes d'adresses IP et les adresses publiques / privées.

> **TP** : Faire effectuer des conversion et des calculs de plan d'adressages. Faire déterminer les adresses de réseau, broadcast et le nombre d'adresses disponibles.

> **TP** : Faire communiquer des machines reliées par un switch sur cisco packet tracer. Faire communiquer les PC de la salle de cour.

III. Les modèles TCP & UDP

Présentation / Explication du modèle TCP et UDP. Mise à disposition si nécessaire du support de présentation.

Explication de la structure des paquets.

IV. Les topologies réseau

Expliquer les différentes topologies réseaux :

- Anneau
- Etoile
- Mesh

Ressources associées :

Réseau - L'adressage IPV4

Réseau - Modèle OSI

Réseau - Entêtes des trames

2.02 - Notions réseaux générales

Durée approximative : ***6h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C04 : Analyser un système informatique***
      - ***Infrastructures matérielles et logicielles centralisées, décentralisées ou réparties***
      - ***Méthodologie de recherche et d'analyse de documentation y compris en anglais***
    - ***C05 : Concevoir un système informatique***
      - ***Infrastructures matérielles***
    - ***C06 : Valider un système informatique***
      - ***Réseaux informatiques (protocoles, équipements et outils usuels et industriels)***
      - ***Sécurisation des réseaux (acl, mots de passe)***
    - ***C09 : Installer un réseau informatique***
      - ***Modèle en couche***
      - ***Protocoles usuels IPv4, TCP/IP, Ethernet, ICMP***
      - ***Routage (incl. NAT et PAT)***
      - ***Commutation (VLAN incl.)***
      - ***ACL***

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R5 : Maintenance des réseaux informatiques***
    - ***C10 : Exploiter un réseau informatique***
      - ***Infrastructure matérielles***
    - ***C11 : Maintenir un réseau informatique***
      - ***Outillage nécessaire au diagnostic, à la réparation et les équipements de rechange***
      - ***Infrastructures matérielles***

> **Conseil** : Inscrire l'ensemble des déroulés des différents TP dans un contexte pro et trouver une continuité dans le scénario pour chaque étape des TP.

I. Adressage IP

Révisions des plans d'adressage, demander pour préparer le TP a avoir les plans d'adressage suivants :

- un réseau de classe A avec 2 machines (/30)
- un réseau de classe B avec 30 machines possibles (/27)
- un réseau de classe B avec 6 machines possibles (/29)
- deux réseau de classe C avec 254 machines possibles (/24)

> **TP1 - Création du 1er réseau** : Création d'un premier réseau avec 1 switch + 4 pc normés, configurés.

Contexte : l'Entreprise Labs404 viens d'ouvrir son premier bureau, il y a 4 employés avec chacun leur poste (2PC fixe et 2 portables). Ils doivent tous pouvoir communiquer pour travailler en réseau.

Configurer le switch (hostname, domaine, horloge, descriptions et emplacement, etc...)

Sécuriser le switch, paramétrage des mots de passe pour chaque niveau d'accès.

II. Routage

Expliquer que sans routage, seul le réseau local est accessible.

Expliquer les bases de fonctionnement du routage (table de routage statique, route par défaut, passerelle par défaut, next hop, TTL)

> **TP** : Faire ensemble des schéma et tables de routage.

> **TP 2 - Ajout de routage local** : Ajout du routeur local et du second réseau.

Contexte : l'Entreprise Labs404 a acquis un nouveau local dans l'immeuble pour développer une seconde activité. Il faut que les deux réseaux communiquent.

III. NAT / PAT & ACL de routage

Pour pouvoir gérer le routage 'internet', il faudra tout d'abord rappeler le concept d'ip publique et ip privée. Puis il faudra également introduire et expliquer le NAT et le PAT en s'appuyant sur les cours correspondants.

> **Conseil** : Utiliser MonIP.org v1.0 pour démontrer l'IP publique.

> **TP3 - Ajout du routage second site + internet** : Ajout de 2 routeurs (1 'internet' et 1 interne vers le réseau 2), ajout du second réseau et de deux PC.

Contexte : La société labs404 doit désormais posséder un accès internet et a acquis un second pool de bureau avec 2 nouvelles personnes. Celui-ci doit être routé en interne.

IV. VLAN & ACL

Expliquer le principe des VLAN et son intérêt du point de vue sécurité. Parler de la logique de Zone, segmentation réseau et zero trust.

Evoquer le risque de 'lateral move' pour appuyer la nécessité de cloisonner ses réseaux en tiers, zones et VLAN.

Expliquer comment s'articulent les tables de VLAN (ID, nom, description, show vlan, ...)

Expliquer le principe et le fonctionnement des ACL.

Le TP sera également l'occasion d'aborder la sécurisation d'un port via la restriction MAC et le 'shut' des ports non utilisés.

> **TP4 - Ajout de VLAN et ACL** : Création d'un VLAN sur site 1 et ajout des ACL pour interdire la com entre vlan 1 & 2.

Contexte : La société Labs404 à acheté deux serveurs qu'elle souhaite prochainement utiliser pour héberger ses services. Il va donc falloir les isoler dans un VLAN à part pour les couper du reste du réseau, il va également falloir un VLAN d'administration depuis lequel un administrateur pourra gérer ces serveurs et le parc, tout en sécurisant l'accès à ceux-ci.

Ressources associées :

<mettre ici les liens vers les pages ressources et support de cours>

2.03 - Protocoles de bases

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R2 : Installation et qualification***
    - ***C06 : Valider un système informatique***
      - ***Réseaux informatiques (protocoles, équipements et outils usuels et industriels)***
      - ***Tests unitaires et d'intégration***
      - ***Fiches de recette (scénario d'utilisation du logiciel, résultats attendus)***
    - ***C09 : Installer un réseau informatique***
      - ***Modèle en couches***
      - ***Protocoles usuels IPv4, TCP/IP, Ethernet, DNS, DHCP***
- ***U5 - Exploitation et maintenance de réseaux informatique***
  - ***R5 : Maintenance des réseaux informatiques***
    - ***C11 : Maintenir un réseau informatique***
      - ***Outillage nécessaire au diagnostic, à la réparation et les équipements de rechange***
      - ***Infrastructures matérielles***

> **Conseil** : Pour familiariser les étudiants avec une approche projet, présenter les TP à travers un projet d'infrastructure et faire valider chaque étape de la mise en place avec des cahiers de recette & tests unitaires.

I. Le protocole DHCP

Expliquer le fonctionnement du DHCP, protocole et configuration.

Principes d'étendues, de réservations, d'exclusion.

> **TP 5 - Ajout du DHCP site 1** : Ajout d'un serveur DHCP sur le vlan1 (par routeur, puis par serveur)

Contexte : La société labs404 va prochainement agrandir son parc de PC et doit se doter d'un DHCP pour ne pas avoir à gérer les adresses du parc.

II. Le protocole NTP

Aborder les problématiques de synchronisation de temps (informations logs erronée, dysfonctionnement kerberos et autres)

Expliquer le fonctionnement du NTP, protocole et configuration.

Montrer un schéma de flux d'une configuration type.

Pool national <-- ntp centraux <-- ntp secondaires (domaine, IoT)

> **TP 6 - Ajout du NTP** : Ajout d'un serveur NTP, synchronisation des temps.

Contexte : La société labs404 va rapidement devoir se doter d'un NTP pour pouvoir installer ensuite ses serveurs d'annuaires.

III. Le protocole DNS

Expliquer le but du protocole dns.

Expliquer son fonctionnement (annuaires, reverse DNS)

Expliquer les différents types de champs DNS

(certains seront vu plus tard vis à vis d'autres protocole, ou sur le passage sur des protocoles sécurisés comme DNSSEC)

> **Conseil** : Parler du cache poisoning, du fichier host local et évoquer l'exfiltration DNS.

> **TP 7 - Ajout des DNS** : Ajout d'un serveur DNS interne.

Contexte : La société labs404 va commencer à intégrer des serveurs et publier du contenu. Aussi, il faut qu'elle soit en mesure de résoudre les noms d'hôtes afin de faciliter la vie de ses utilisateurs.

A la fin des TP, un fichier CPT pourra être fourni à titre d'exemple contenant l'ensemble de l'infrastructure et la partie internet avec des services externes, internes et une "box" qui fait le lien.

Ressources associées :

Réseau - Le protocole DNS

3.01 - Introduction au développement

Durée approximative : ***8h***

Eléments du référentiel adressé :

- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R4 : Gestion de projet et d'équipe***
    - ***C03 : Gérer un projet***
      - ***Méthodes de conduite de projet (Agile Scrum, Kanban, Cycle en V)***
- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D2 : Développement et validation de solutions logicielles***
    - ***C06 : Valider un système informatique***
      - ***Ingénierie logicielle (UML)***
    - ***C08 : Coder***
      - ***Spécificités des environnement de développement, de test, de production***
      - ***Outils de modélisation***
      - ***Outils de documentation***

I. Les types de langages

Aborder et décrire les différents types de langages :

- Procéduraux (batch, basic, etc...)
- orienté objet (Powershell, python, C++)
- Descriptif (YAML, JSON, XML)
- Web (html, css)
- BDD (SQL)

Indiquer le niveau de maîtrise attendu pour chaque type et contextualiser leur utilisation.

II. Les bonnes pratiques en développement

Expliquer la nécessité de bien commenter et documenter son code. Notamment dans un contexte de travail collaboratif.

Aborder la normalisation sur les scripts (Powershell par exemple, avec les en-têtes, sections, etc...)

Introduire les logiques de DevSecOps. La méthode agile vs cycles en V.

Expliquer le cycle dev to prod avec les différents environnements : DEV --> UAT --> PROD

III. La logique algorithmique

Réfléchir au langage le plus adapté au besoin

Faire dérouler un processus simple.

Introduire progressivement les élément conditionnel :

- if
- if,else
- if,then if, elif
- switch, cases

Introduire les boucles :

- for, foreach
- while, do while, do until

> **TP** : commencer sur un notepad ou un vscode à faire écrire des programmes simples en langage naturel.

> **Conseil** : Pour faire intégrer la logique d'évolution du code, procéder au développement de manière itérative en faisant évoluer le besoin de base. De plus, pour évoquer le besoin, passer par des diagrammes UML/SYSML si possible.

IV. Recherche de documentation

Expliquer comment rechercher la documentation sur les langages.

A travers les Man pages (local ou en ligne) et les documentations éditeurs.

Ressources associées :

<n/a>

4.01 - Introduction à la gestion de projet

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R1 : Accompagnement du client***
    - ***C01 : Communiquer en situation professionnelle***
      - ***Communication écrite : cahier des charges, dossiers de présentation***
- ***U5 - Exploitation et maintenance de réseaux informatiques***
  - ***R4 : Gestion de projet et d'équipe***
    - ***C01 : Communiquer en situation professionnelle***
      - ***Communication écrite : cahier des charges, dossiers de présentation***
    - ***C02 : Organiser une intervention***
      - ***Différents acteurs du projets : sous-traitants, clients, maître d'œuvre, maître d'ouvrage, utilisateurs, exploitants, etc...***
    - ***C03 : Gérer un projet***
      - ***Méthodes de conduite de projet (Méthodes Agile Scrum, Kanban, cycle en V)***
      - ***Outils de gestion de projet***
      - ***Différents acteurs du projets : sous-traitants, clients, maître d'œuvre, maître d'ouvrage, utilisateurs, exploitants, etc...***

I. Les étapes clé du projet

> **“ Parce que l'informatique commence sur le papier.**
>
> *- source inconnue*

Un projet peut se découper en 4 grosses étapes, elles-mêmes scindées en sous-étapes avec chacune leurs objectifs et étapes de validation. Mais si il faut ne retenir que les étapes principales :

1. Démarrage / Lancement de projet
2. Planification

3. Exécution
4. Clôture

Toutes ces étapes seront accompagnées d'un processus de surveillance et de maîtrise pour vérifier que le projet se déroule bien et palier aux potentiels problèmes.

> **Conseil** : Donner accès aux étudiants à la ressource ci-jointe et la parcourir avec eux.

II. Analyse d'un Premier cahier des charges

Il s'agit d'échanger avec le client sur son projet, d'élaborer la charte projet, le cahier des charges et d'identifier tout ce qui sera nécessaire à son étude et sa conception. Moyens humains et matériels à mettre en œuvre.

Définition des acteurs du projets :

- Sous-traitants
- Clients
- Maître d'œuvre
- Maître d'ouvrage
- Utilisateurs
- Exploitants
- Chef de projet

Fournir et étudier les documents suivants :

- Cahier des charges
- Demande d'intervention client
- Schémas d'infrastructures
- DAT de l'existant

> **TP** : A partir des documents, identifier le besoin, les intervenants.

III. Méthodes de conduite de projets

Présenter en détail et fournir des supports pour les différentes méthodologie de gestion de projets, en présenter les éléments et en définir les termes :

- Agile
- Kanban
- Scrum
- Cycle en V

Expliquer les pour/contres de chaque méthode et préciser en quoi elles sont adapter plus à tel ou tel type de projet.

IV. Outils logiciels pour la conduite de projet

Présenter les outils logiciels pour la conduite de projet :

- MS Project
- MS Visio / Draw.io
- Modelio

La pratique sur ces outils se fera tout au long de la formation.

Ressources associées :

Méthodologie - Définition des termes (méthode agile)

5.01 - Introduction à la cybersécurité

Durée approximative : ***2h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R1 : Accompagnement du client***
    - ***C04 - Analyser un système informatique***
      - ***Acteurs de l'écosystème réglementaire, normatif et de référence des bonnes pratiques***
      - ***Méthodologie de recherche et d'analyse de documentation y compris en anglais***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D1 : Elaboration et appropriation d'un cahier des charges***
    - ***C05 -Concevoir un système informatique***
      - ***Usages et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

I. Le paysage de la cybersécurité

Définir les types de hacker.

- White hat
- Grey hat
- Black hat

Faire un tour d'horizon des sources de menaces :

- cybercriminalité (extorsion de fond, destruction brute, activités de réseau)

- terrorisme (risques terrorise et écoterroriste, militants écologiques ou politiques, attaque sur des infrastructures vitales)
- Espionnage industriel ou étatique (concurrent malveillant ou puissance étrangère)
- Cyberguerre (acte de guerre de la par d'une puissance étrangère)

Evoquer l'industrialisation de la menace. Le fait que les actions sont de moins en moins commises par des pirates isolées, mais de plus en plus par des réseaux structurés, utilisant principalement des robots et des méthodes d'industrialisation des attaques.

> **Conseil** : illustrer le propos avec des captures de trames ou des logs de pare feu sur une interface publique.

> A titre individuel, lorsque je faisais de l'hébergement chez moi (2023 à 2025), c'était en moyenne 400 à 600 tentatives par jours. Essentiellement des actions automatisées à large échelles, effectuées par des robots qui scannaient à longueur de temps la moindre faille. Ce n'est qu'en cas de succès de ces opérations qu'un humain prends la relève.
>
> *- Chabran Olivier*

Terminer sur les objectifs des pirates, les deux principaux sont :

- Voler ou extorquer de l'argent
- Rendre des services inaccessibles ou inopérants
- Voler des données confidentielles, qui aujourd'hui, valent bien plus que l'argent en lui même.

II. Les principales attaques

> **Une chaîne n'a que la force de son maillon le plus faible.**

> *- Olivier Lajous, "L'art de diriger ?"*

De nombreuses attaques ciblent les systèmes. Les principales qui ciblent les systèmes sont :

- Attaque par DDoS
- tentatives d'intrusion
- ransomwares

Mais vu que les systèmes sont de plus en plus protégés, la cible privilégiée est l'élément humain : l'utilisateur

- Phishing
- Malwares
- ransomware
- Social engineering

Concernant les vecteurs d'attaques (messagerie, wifi public, clé USB), présenter les vecteurs et leur méthodologie d'exploitation.

> **Conseil** : Utiliser des échantillons de mails, un résultat de scan wifi wireshark et des clé USB pour illustrer le propos.

Expliquer les méthodes de préventions utilisées pour la correction de ses points.

- Campagnes de phishing
- Politique de traitement des clé USB trouvées
- utilisation d'un VPN, préférer les partages de connexion 4G au wifi public si possible.

III. Le rôle grandissant de l'IA dans la cybersécurité

Evoquer l'utilisation de l'IA dans la recherche et la protection des menace.

Evoquer également son pendant en terme de développement et d'automatisation des attaques utilisé par les pirates.

IV. Les acteurs règlementaires et normatifs

En réponse aux menaces et aux dérives quand au traitement de la donnée par les GAFAM et autres, une série d'organisme a vu le jour.

Ceux-ci sont en charge de gérer les aspects règlementaires, législatifs et normatif quand à la sécurité informatique et le traitement des données.

- CNIL
- ANSSI
- Cybermalveillance
- CVE Foundation
- CERT-FR

> **TP** : Sur le site de l'anssi, chercher et télécharger les guides de bonnes pratiques. Analyse et débat en classe.

Conclure sur le rôle de "white hat" de l'étudiant.

> **Evaluation** : faire signer le contrat de prestation cyber aux étudiants.

Ressources associées :

Les types de hackers et principes d'attaques

Etat des cybermenaces (2025)

5.02 - Analyse de risque et bonnes pratiques en cybersécurité (CIEL)

Durée approximative : ***4h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R1 : Accompagnement du client***
    - ***C04 : Analyser un système informatique***
      - ***Acteurs de l'écosystème réglementaire, normatif et de référence des bonnes pratiques***
      - ***Méthodologies d'analyse de risque***
      - ***Méthodologie de recherche et d'analyse de documentation, y compris en anglais***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D5 : Audit de l'installation ou du système***
    - ***C03 : Gérer un projet***
      - ***Moyens, outils et méthodes permettant d'effectuer une veille technologique***
    - ***C10 : Exploiter un réseau informatique***
      - ***Usage et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

I. Les recommandations et bonnes pratiques

Suite au TP de l'introduction, les étudiants doivent avoir téléchargé les guides de bonnes pratique et en avoir un résumé assez clair.

Lien de téléchargements :

- EXT - anssi : règles d'or
- EXT - anssi : bonnes pratiques

Il peut être bon d'afficher les fiches de synthèse dans la classe.

Pour chaque point suivant, expliquer avec des exemple et leur demander une analyse de risque basique :

1. Mots de passe forts uniques (brute force, attaque par dictionnaire, fuite de donnée, ...)
2. Garder les systèmes à jour (failles, zeroday, ...)
3. Effectuer des sauvegardes régulières, si possible offline et externalisées (incendie, cryptolocker, ...)
4. Réfléchir avant de cliquer (l'attaquant crée une situation d'urgence pour nous berner)

II. Analyse de risque cybersécurité

2.1 La norme ISO27001

Présenter rapidement la norme ISO 27001, son historique et son but en s'appuyant sur : EXT - Wikipedia : iso 27005

2.2 La méthode EBIOS

Que cela soit pour un audit de sécurité ou pour une analyse interne, il est important de savoir évaluer correctement le risque sécu et qualifier le niveau de menace.

S'appuyer sur les documents de l'anssi pour organiser les ateliers : EXT - anssi : Methode ebios

> **TP** : dérouler les ateliers présentés dans le document de l'anssi et le mettre en parallèle avec le projet à venir.

III. Les outils de veille

Présentation des outils de veille et des bulletins CERT-FR. Lecture d'un ou deux exemple.

Explication de la nécessité de disposer d'outils de veille technologique, notamment les flux RSS de l'anssi et de la cnil.

Etendre cette veille aux aspect technologiques, ne pas négliger les réseaux style LinkedIn ou des agrégateurs d'actualité.

- Flux RSS anssi : https://www.cert.ssi.gouv.fr/feed/
- Flux RSS CNIL : https://www.cnil.fr/fr/rss.xml

> **Conseil** : il sera utile plus tard de mettre en place ces flux dans GLPI par exemple.

> **TP** : mise en place de flux RSS sur teams ou discord.

Supports de cours associés :

- Sécurité - Analyse de risque (méthode Ebios)

Ressources associées :

- *Solidité mots de passe (2025)*
- *Evaluation des risques cybersécurité*
- *Méthodologie - Méthode PDCA*

5.03 - Stratégies de sauvegardes, PCA/PRA et DRP (CIEL)

Durée approximative : ***2h***

Eléments du référentiel adressé :

- ***U5 - Exploitation et maintenance de réseau informatiques***
  - ***R5 : Maintenance de réseau informatiques***
    - ***C10 : Exploiter un réseau informatique***
      - ***Politique et outils de sauvegarde***
- ***U6 - Cybersécurité et valorisation de la donnée***
  - ***D4 : Valorisation de la donnée***
    - ***C08 : Coder***
      - ***Politiques de sauvegarde/restauration des données***

I. Stratégies de sauvegarde

Les différentes stratégies de sauvegardes (différentiel, incrémentiel, complète, etc...).

Parler des pertes sur restauration. De la nécessité d'avoir des sauvegardes offline (cryptolocker) et externalisées (risque physiques).

II. Stratégies de PCA

Définir le PCA, expliquer son contexte et sa mise en œuvre.

Donner les exemples (matériel redondé, RAID).

Stratégie de réplication de VM, Clustering.

> **Conseil** : Donner en exemple le datacenter tier 4 de chez HPE à Grenoble.

III. Stratégie de PRA

Définir le PRA, expliquer son contexte et sa mise en œuvre.

Parler du site de PRA. Définir les contraintes de mise en œuvre.

Notamment financière avec les coûts exponentiel pour augmenter la disponibilité et les contraintes en terme de sélection de zone.

- Pas dans un couloir aérien
- Normes parasismiques, zone de risque sismique et éboulements

Table des distances - risques naturels et anthropiques

Dans la conception d'un centre de données, le choix du site est l'une des étapes les plus cruciales et constitue la toute première étape. Nous nous concentrons principalement sur deux sous-domaines : les risques naturels et anthropiques.

Objet fabriqué par l'homme	Distance minimale (KM)
Stations-service/carburant	1.6
Lignes de transmission à haute tension	1.6
Les fugues des aéroports	1.6
Petits lacs et zones de débordement	1.6
Chemins de fer	1.6
Grand complexe de magasins	1.6
Tours de stockage d'eau	1.6
Canaux	3.2
Ports et ports	3.2
Lacs et barrages	3.2
Carrières	3.2
Stations radar	5

Laboratoires de recherche	5
Stations de radio/télévision	5
Ambassades	5
Aéroports	8
Usines chimiques et électriques	8
Stations et installations militaires	13
centrales nucléaires	80

III. Stratégie de DRP

Définir le DRP, expliquer son contexte et sa mise en œuvre.

Expliquer l'intérêt de conduire régulièrement des exercices de DRP avec un cahier de recette.

> **Idée TP** : Pour chaque thème, faire proposer un plan adapté au besoin de leur entreprise.

> Réaliser un cours compte rendu intégrant les aspect normatifs et réglementaires et justifiant la pertinence des stratégies. Faire ensuite comparer les stratégies entre eux.

> Proposer une simulation de 'disaster recovery'.

Cours associés :

Sécurité - La sauvegarde

Sécurité - PCA, PRA et DRP

Ressources associées :

Infrastructure - Les tiers de datacenter