

# Bloc de compétences 3 : Cybersécurité des services informatiques

- Présentation du Bloc 3 1ère année
- Présentation du Bloc 3 2ème année

## B3.1 : Protéger les données à caractère personnel

### Chapitre 1 : Identifier les risques liés aux données à caractère personnel

- Les traitements sur les données à caractère personnel
- Présentation du contexte Centrecall
- Fiche savoirs technologiques : découvrir JMOT
  - Ressource : registre des traitements
- PIA : Analyse d'impact relative à la protection des données
- RGPD : les étapes nécessaires à la mise en conformité

### Chapitre 2 : Appliquer et diffuser la réglementation liée aux données à caractère personnel

- Préparer le serveur de BDD
- Gestion des habilitations de la base de données
- Conseils pour réaliser un diaporama

## B3.2 : Préserver l'identité numérique de l'organisation

- Présentation du contexte M@Banque
- Configurer une messagerie sécurisée avec Mozilla ThunderBird
- Visualiser avec Wireshark les échanges chiffrés avec les serveurs IMAP et SMTP
  - Cours : Communiquer sur un réseau Ethernet - TCP/IP Document étudiant
  - Activité d'analyse de trame
- Activité : Etude de la commande ping et du protocole HTTP (Web) avec l'analyseur de protocoles wireshark
  - Cours Préserver l'identité numérique - risques de cyberattaques
  - TD Préserver l'identité numérique - risques de cyberattaques
- Fiche savoirs : l'authentification forte
- Accès à distance avec Telnet et SSH
- Activité sur l'accès à distance SSH et l'authentification avec une clé SSH
- Utiliser la solution de virtualisation Proxmox avec des conteneurs LXC
  - Les outils d'une veille technologique

### Kali

- Le contexte BOXTOBED

Préparer l'environnement de test :

- Fiche savoirs technologiques : Prise en main et configuration initiale du SNS
- Fiche savoirs technologiques : Mise en place du plan d'adressage réseau du Lab
- Le besoin de chiffrement des flux

## B3.3 : Sécuriser les équipements et les usages des utilisateurs

- Le BYOD
- Activité : connaître les menaces
- Fiche savoirs : l'authentification forte
- Activité : authentification forte et FIDO 2
- Vérifier l'intégrité d'une ressource
  - Explorer le chiffrement des fichiers et des données  
Fichier PT
  - Utiliser des vérifications d'intégrité des données et des fichiers  
Fichier PT
- Fiche savoirs : les différents profils de cybercriminel
- Activité : Audit sur la sécurité des identifiants avec Kali (avec une VM Windows 10)

- Activité : Audit sur la sécurité des identifiants avec Kali (sans VM Windows 10)
- Activité : Identifier les menaces et mettre en oeuvre les défenses appropriées
- Fiche savoirs : le contrôle des accès
  - Activité : authentification, autorisation et journalisation
    - Activité Labtainer : les sauvegardes
    - Activité Labtainer : chiffrement symétrique
- Activité : connaître les attaques informatiques
- Activité : la dissimulation de données
- Fiche savoirs : les trois principes de sécurité - CID
- Fiche savoirs : l'intégrité des données
  - Fiche savoirs : Incidents réseau
  - fiche\_technologique\_utiliser\_portqry.pdf
  - fiche\_technologique\_installer\_et\_utiliser\_portqry\_pour\_ad.pdf

### **B3.4 : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques**

#### **Etudier les menaces et les vulnérabilité d'un réseau**

- Prise en main des outils de diagnostic du réseau avec Labtainer
  - Fiche savoir : Structure d'une trame Ethernet et d'un datagramme IP  
Doc odt
- Fiche savoir : la fragmentation IP
- Fiche savoir : Les connexions TCP
- Fiche savoir : Le protocole UDP
- Activité : Etude du protocole DHCP avec Wireshark
  - Activité : observer le handshake TCP avec Wireshark  
Document docx
- Fiche savoirs : Le centre opérationnel de sécurité

### **B3.5 A : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service (option A)**

- Mise en oeuvre de l'UTM Stormshield
- Le contexte BOXTOBED
- Vérifier l'intégrité d'une ressource
- Le besoin de chiffrement des flux
- Exploitation d'une faille applicative via Metasploit
- Activité : améliorer la disponibilité

#### **Sécuriser des données ou des échanges avec des solutions de chiffrements**

- Cryptographie - chiffrement symétrique
- Chiffrez les données d'un fichier ou d'une clé USB
- Cryptographie - chiffrement asymétrique
- Configurer une authentification avec un couple de clés privée/publique SSH
- Activité Root-Me sur le chiffrement
  - Cryptographie - Fonction de hachage
- Activité : Configurer les accès Wifi de manière sécurisée
  - Cryptographie - signature numérique et chiffrement
    - PKI - Infrastructure à clés publiques
- Activité : Configurer une PKI pour gérer des certificats utilisateurs et serveurs
  - Cours : VPN IPsec
  - Fiche savoirs 12 : Le VPN
- Activité : configurer un VPN SSL entre deux contextes
- Activer le routage avec Linux Debian
  - Cours iptables
  - Activité Iptables
  - Schéma réseau

From:

[/- Les cours du BTS SIO](#)

Permanent link:

</doku.php/bloc3s1/accueil?rev=1670317971>

Last update: **2022/12/06 10:12**

