UTC505 - Introduction à la cyberstructure de l'internet - réseaux et sécurité

Les pré-requis

- Une culture de base en systèmes d'exploitation, en programmation et en mathématiques telle que demandée dans un DUT informatique.

- À défaut :
  - S'inscrire sur OpenClassRoom et suivre le Mooc : Concevez votre réseau TCP/IP
  - Lire les pages de Wikilivres - Les réseaux informatiques (ou le PDF : Les réseaux informatiques

Plan indicatif du cours - UTC505

1 - Architecture logicielle des réseaux

Diviser pour régner ; modèle en couches OSI vs Internet ; encapsulation

- Découverte de l'architecture de communication en couches. Du modèle OSI à l'architecture Internet; introduction à l'outil d'analyse de traces Wireshark.
  - Architecture logicielle des réseaux
  - Définitions
  - Le modèle de référence OSI ; présentation des couches ; encapsulation
  - L'architecture TCP/IP

2 - Couche réseau

Carrefours, itinéraires et destinations

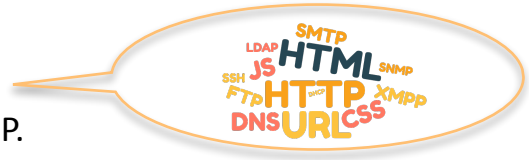
- Adressage, tables de routage et l'expédition de données dans le réseau IP. Evolution de IPv4 à IPv6.
  - Objectif de la couche réseau
  - Algorithme de routage
  - Interconnexion de réseau
  - La couche Internet (présentation, Le protocole IP, Les adresses IPv4, Sous-réseau IPv4, Adresses particulières & adressage privé, Configuration IPv4 des hôtes, autres protocoles, IPV6)

3 - Couche transport

Une lettre ou un appel ?

- Transport de données entre un client et un serveur à travers UDP et TCP avec le modèle datagramme, et les approches connecté et non connecté. Gestion et utilisation de l'API socket.
  - Objectifs de la couche transport
  - Les protocoles de transport
  - La couche Transport dans Internet (Socket, ; TCP : en-tête, connexion, Gestion de la connexion TCP, Fenêtre d'anticipation TCP & gestion des congestions. UDP)

4 - La couche application



- La couche application de l'architecture TCP/IP.
- Introduction à quelques protocoles ; HTTP ; DNS

Course d'obstacles en tous genres

5 - Les boitiers divers et variés; « middleboxes »

- Étude de l'impact des équipements NAT, firewall, etc.

6 - La sécurité

Où sont les clefs ?

- Introduction à la sécurité
  - Bonnes pratiques de sécurité personnelle
  - Droit du numérique
  - Côté entreprises : normes et règlementation
- Menaces
  - Études de cas d'attaques : Stuxnet, TV5Monde, fraude au président (Pathé), etc.
  - Rançongiciels : Colonial Pipeline, HSE, Kaseya VSA
  - Processus d'attaque : MITRE ATT&CK Framework, Unified Kill Chain, menaces persistantes avancées (APT)
- Mesures de sécurité
  - Vulnérabilités : failles 0-day, échelle de sévérité, CVE MITRE, score CVSS
  - Déploiement des correctifs de sécurité. Séparation des environnements.
  - Scan de vulnérabilités, durcissement de configuration, vérification de la conformité technique
  - Modélisation des menaces
  - Sécurité du code pour les développements logiciels : débordement de tampon ou d'entiers, MITRE CWE. Bonnes pratiques de développement et d'amélioration de la qualité du code. Fuzzing, tests d'intrusion, exercices red/blue team.
  - Impacts : bilan d'impact sur l'activité (BIA), temps et point de rétablissement (RTO et RPO), Data Protection/Privacy Impact Assessment (D)PIA, plans de reprise (PRA), de continuité (PCA), d'urgence et de poursuite d'activité (PUPA)
  - Gestion des risques informatiques : ISO 27000, méthodologies EBIOS et MEHARI
  - Organisation de la sécurité : SOC, surveillance des événements de sécurité (SEM)
  - Sensibilisation des utilisateurs à la sécurité informatique
  - Sécurité des authentifications : biométrie, mots de passe, possession. Authentification forte multi-facteurs.
  - Défense en profondeur, modèle du château fort, dépérimétrisation de l'infrastructure informatique et réseaux 'zéro trust'
- Primitives cryptographiques
  - Propriétés de sécurité, de contrôle d'accès et de sûreté de fonctionnement
  - Approches historiques : codage, stéganographie, chiffrement
  - Principe de Kerckhoffs
  - Taxinomie des techniques de cryptanalyse : KPA, CPA, CCA.
  - Niveau de sécurité
  - Analyse des fréquences (Al-Kindi). Indice de coïncidence de Friedman
  - Algorithmes historiques : César, Vigenère, Playfair, ADFGVX, Enigma.
  - Sécurité inconditionnelle de l'algorithme du masque à usage unique (chiffre de Vernam)
  - Principe des chiffres symétriques (en continu ou par blocs) et à clé publique.
  - Cryptosystèmes hybrides. Infrastructures de clés publiques et autorités de certification.