CERTIFICAT EN SÉCURITÉ DANS LES RÉSEAUX INFORMATIQUES

1. Responsables du certificat

- Pr Alassane DIOP, enseignant-chercheur (UVS)
- Pr Mohamed MEJRI (Université Laval), enseignant-associé
- Mr Pape Moussa Ndiaye (Consultant en sécurité, Genève, Suisse)
- Mr Calvin Nangue (Formateur Cisco)
- Mme Ndèye Fambaye NIANG (Informaticienne, Technopédagogue) (UVS)

2. Objectifs

Objectif général

Cette certification permet aux apprenants d'avoir de solides bases en réseaux informatiques et de comprendre les cyber-attaques pour mieux se défendre.

Objectifs spécifiques :

A l'issue de ce cours les apprenants seront en mesure de :

1. Planifier et concevoir un réseau : Établir un système d'adressage IP ;
2. Mettre en œuvre, faire fonctionner et dépanner un réseau informatique ;
3. Évaluer un processus de communication TCP/IP (Transmission Control Protocol / Internet Protocol) et de ses protocoles associés ;
4. Maîtriser la démarche suivie par les pirates pour mener des attaques ;
5. Comprendre les principaux vecteurs d'attaques utilisés par les pirates ;
6. Découvrir les principales vulnérabilités des applications Web ;
7. Démystifier la sécurité des réseaux sans fil ;
8. Expérimenter les principaux outils de détection et l'exploitation de vulnérabilités (Wireshark, maltego, nmap etc.) ;
9. Savoir comment se défendre des cyber-attaques ;
10. Gérer les risques ;
11. Pratiquer le plan de continuité d'activité ;
12. Sécuriser les réseaux.

3. Cibles

Technicien et ingénieurs en informatique

4. Description et/ou agencement du programme

INTRODUCTION AUX RÉSEAUX INFORMATIQUES

1. Présentation des réseaux
   a. Composants de l'ordinateur
   b. Connexion physique pour relier les ordinateurs
2. Aspects mathématiques des réseaux
   a. Présentation binaire des données
   b. Présentation hexadécimale des données
   c. Logique booléenne
   d. Adresse IP et masques de réseau
3. Notions de bases des réseaux
   a. Terminologie des réseaux
   b. Définition de bande passante
   c. Différents modèles de réseau
4. Médias réseaux
   a. L'aspect électricité
   b. Les câbles
   c. Les connecteurs
   d. La fibre optique

SECURITE DES RESEAUX INFORMATIQUES

1. Reconnaissance de la cible
   a. Footprinting
   b. scanning
   c. Enumération
2. Vecteurs d'attaques
   a. Accès physique direct à un ordinateur
   b. Ingénierie social
   c. Service Réseaux

d. Authentification
e. Débordement de tampons
f. Serveurs et applications Web

3. Sécurité des réseaux sans fil
   a. Techniques de protection
   b. Vecteur d'attaques

GESTION DES RISQUES

1. Introduction aux risques
   a. Pourquoi la gestion des risques
   b. Les définitions
   c. La démarche
   d. Une norme pour tous
2. Risques SSI (critère DIC, organisation, métiers..) et définitions
3. Les risques liés au système informatique et l'ISO
   a. Les concepts fondamentaux
   b. Les normes ISO 27000 et le modèle SMSI
   c. L'analyse de risques dans la norme ISO 27001
   d. La norme 27005
4. Les méthodes publiées
   a. iso 27005,
   b. Mehari,
   c. Ebios,
   d. Owasprisk…..
5. Etude de cas complète

PLAN DE CONTINUITÉ D'ACTIVITÉ

1. Avoir une vision globale du risque
2. Identifier les enjeux pour une entreprise
3. Acquérir des concepts fondamentaux de l'analyse de risques
4. Avoir une démarche complète pour mener à bien un projet d'analyse de risques
5. Avoir une approche normative d'un SMSI ISO27000
6. Panorama des méthodes d'analyse de risques et des solutions logicielles
7. Communication

CONCEPTS DE SÉCURITÉ DES RÉSEAUX

1. État actuel de la cybersécurité
   a. Décrire l'état de la cybersécurité aujourd'hui et les vecteurs des pertes de données.
2. Acteurs
   a. Décrire les outils utilisés par les acteurs de menace pour attaquer les réseaux.
3. Logiciels malveillants
   a. Décrire les types de logiciels malveillants.
4. Attaques réseau courantes
   a. Décrire les attaques réseau courantes.
5. Menaces et vulnérabilités liées au protocole IP
   a. Expliquer comment les vulnérabilités liées au protocole IP sont exploitées par les acteurs de menace.
6. Vulnérabilités liées aux protocoles TCP et UDP
   a. Expliquer comment les vulnérabilités liées aux protocoles TCP et UDP sont exploitées par les acteurs de menace.
7. Services IP
   a. Expliquer comment les services IP sont exploités par les acteurs de menace.
8. Meilleures pratiques de sécurité réseau
   a. Décrire les meilleures pratiques de protection d'un réseau.
9. Cryptographie
   a. Décrire les processus cryptographiques courants utilisés pour protéger les données en transit.

CONCEPTS DE VPN ET IPSEC

1. Technologie VPN
   a. Décrire les avantages de la technologie VPN.
2. Types de VPN
   a. Décrire différents types de VPN.
3. IPsec
   a. Expliquer comment la structure IPsec est utilisé pour sécuriser le trafic réseau.

ATELIERS PRATIQUES SECURITE DES RESEAUX D'ENTREPRISE

5. Modalités d'évaluation

- Évaluation théorique sur les acquis
- Évaluation par un projet pratique

6. Conditions d'admission

Avoir au minimum un bac+2.

7. Durée de la formation

6 mois

8. Tarifs

300.000 F CFA

Contacts : Pour toute demande d'informations, adresser un mail à l'adresse suivante : **certificat.admission@uvs.edu.sn**