

SECURITE INFORMATIQUE ET RESEAU (SIR)

formationfacile.hitt.tg@gmail.com

1^{ère} Edition

SIR : Sécurité Informatique et Réseau

Pour la sécurité des systèmes informatiques et réseaux

A l'usage des BTS, Licence et Master

HIT-TECHNOLOGY SARL U

SECURITE INFORMATIQUE ET
RESEAU (SIR)

COURS et EXERCICES CORRIGES

Formateur en développement applicatif

Enseignant à l'Université de Lomé et dans les Institutions privées (Togo)

Fondateur du Cabinet HIT-TECHNOLOGY SARL U

Alassani AKANATE

a.daviman@gmail.com

E-Book : www.services.hittechnologie.com

Tel : (+228) 97 31 77 52 / 93 32 77 18

01 BP : 1341 Lomé-Togo.

« L'avenir de l'Homme se trouve dans sa manière de penser »

L'équipe HIT-T

© *Tous droits réservés 2026 HIT-T*

DANS LA MÊME COLLECTION

1	ARCHITECTURE ET INTERCONNEXION RESEAU
2	SGBD MySQL ET SQL
3	ANALYSE ET CONCEPTION DES SYSTEMES D'INFORMATION (ACSI) AVEC MERISE
4	SGBD MICROSOFT ACCESS 2010
5	SGBD MICROSOFT EXCEL 2007-2010 (Excel débutant, intermédiaire et avancé)
6	SQL POUR MySQL ET ORACLE
7	SE-OS, CONFIGURATION ET SECURITE
8	SECURITE INFORMATIQUE ET RESEAU
9	INFORMATIQUE ET CONFIGURATION
10	OFFICE 2007-2010 ET INITIATION (Word-Excel-PowerPoint-Publisher)
11	DEVELOPPEMENT DE SITES WEB AVEC LE CMS/SGC JOOMLA ET LES BASES DE DONNEES MySQL
12	P.O.O. : Java SE
13	P.O.O. : C++ et Qt
14	Ecrits Professionnels (EP)
15	Droit Social et de Travail (M. ALASSANI)
16	Economie Générale (M. AMANA)
17	Santé, Sécurité et Hygiène au travail (S. S. H. T.)
18	Tenue de caisse – Facturation
19	Electronique dans l'automobile
20	Climatisation dans l'automobile
21	MS SQL SERVER 2012-2014 et SQL / T-SQL
22	LES TECHNOLOGIES xDSL (Techniques d'accès à l'Internet)
23	MIEUX PARLER ANGLAIS
24	DROIT, NEGOCIATION ET CONTRATS INFORMATIQUES
25	SOCIAL MEDIA – NETWORKING (Marketing digital)
26	BLOCKCHAIN ET LES CRYPTO ACTIFS

TABLE DES MATIERES

TABLE DES MATIERES.....	2
A QUI S'ADRESSE CE LIVRE.....	8
PREREQUIS	8
POURQUOI CE LIVRE ?.....	8
OBJECTIFS SPECIFIQUES DE CE LIVRE.....	8
A PROPOS.....	8
INTRODUCTION GENERALE.....	10
CHAPITRE I : GENERALITES, DEFINITIONS ET CONCEPTS SUR L'INFORMATIQUE, L'OUTIL INFORMATIQUE ET RESEAU	11
INTRODUCTION.....	12
1. Informatique	12
1.1. Système	12
1.2. Système Informatique (ou SI)	12
1.3. Système d'information (SI) ou (information system IS).....	13
1.4. Le système d'exploitation (SE, en anglais Operating System ou OS).....	13
1.5. Programme informatique.....	13
1.6. Logiciel.....	13
1.7. Virus informatiques	13
1.8. Antis virus	14
1.9. L'ordinateur.....	14
2. Structure de l'ordinateur.....	14
2.1. Le Hardware (matériels).....	15
2.2. Le Software (Logiciel)	16
2.2.1. Les systèmes d'exploitation	16
2.2.1.1. Les systèmes d'exploitation sur le marché	16
2.2.1.2. Les SE et les réseaux informatiques	17
2.2.2. Les logiciels d'application.....	17
CONCLUSION	17
CHAPITRE II : MENACES ET OUTILS DE SECURITE INFORMATIQUE ET RESEAU	19
INTRODUCTION.....	20
1. Pourquoi la sécurité ?	20
2. Différentes catégories de problèmes de sécurité et les mesures à prendre	20

2.1.	Catégories de problèmes de sécurité	21
2.2.	Mesures à prendre.....	21
3.	Menaces et risques.....	22
3.1.	Menaces passives.....	22
3.1.1.	Cheval de Troie	22
3.1.2.	Mystification (Spoofing)	22
3.1.2.1.	ARP Cache Poisoning.....	22
3.1.2.2.	IP Spoofing	22
3.1.2.3.	DNS Cache Poisoning ou Attaque par l'ajout de plusieurs résolutions (Kashpureff - 1997)	23
3.1.3.	Ecoute des connexions (sniffing)	24
3.2.	Ecoute Passive	24
3.3.	Menaces actives.....	24
3.3.1.	Déni de Service (DoS).....	24
3.3.1.1.	Objectif du DoS.....	24
3.3.1.2.	DoS par saturation des ressources	25
3.3.2.	Techniques d'intrusion	25
3.3.2.1.	Attaque par usurpation d'identité	26
3.3.2.2.	Piratage par rebond	26
3.3.2.3.	Sites clandestins et sites relais.....	27
3.3.2.4.	Intrusion physique, Social Engineering	27
3.3.3.	DDoS : Distributed DoS	27
3.3.4.	Attaques TCP SYN.....	27
3.3.5.	Recherche de mot de passe.....	27
4.	Agression - Motivation et conséquences	28
5.	Conséquences d'une sécurité insuffisante.....	28
6.	Facteurs d'insécurité	29
6.1.	L'humain & sa machine	29
6.2.	Programme malveillant (Malware).....	30
6.2.1.	Cheval de Troie (trojan).....	30
6.2.2.	Vers informatiques	31
6.2.3.	Autres Vers	31
6.2.4.	Espions – Spyware	32
6.2.5.	Enregistreur de frappe (keylogger)	32

6.2.6.	Portes dérobées : backdoor	33
6.2.7.	Courrier électronique	33
6.2.8.	Canular Informatique (hoax)	33
6.2.9.	Spam	33
6.2.10.	L'hameçonnage (phishing).....	34
7.	Services de sécurité	34
7.1.	Confidentialité	35
7.2.	Identification et authentification.....	35
7.3.	Contrôle d'accès	35
7.4.	Intégrité	36
7.5.	Disponibilité	36
7.6.	Non répudiation.....	36
8.	Cryptographie.....	36
8.1.	Définitions – Terminologie	37
8.2.	Algorithmes de cryptographie	37
9.	Techniques fondamentales de conception des algorithmes	37
9.1.	Transposition	37
9.2.	Substitution.....	38
10.	Chiffrements des données.....	38
10.1.	Chiffrement symétrique des données	38
10.1.1.	DES (Digital Encryption Standard).....	39
10.1.2.	Le nouveau Standard AES.....	40
10.1.2.1.	Historique.....	40
10.1.2.2.	Advanced Encryption Standard (AES) : Caractéristiques.....	40
10.1.2.3.	AES : Rijndael.....	40
10.1.2.4.	Rijndael versus DES	41
10.2.	Chiffrement asymétrique des données.....	41
10.2.1.	Objectif.....	43
10.2.2.	Caractéristiques	43
10.2.2.1.	RSA : fonctionnement.....	43
10.2.2.2.	Le crypto système RSA.....	43
11.	Fonctions de hachage	44
11.1.1.	Hachage: propriétés désirées	44
11.1.2.	Exemple de fonction de hachage :.....	45

12.	Signature électronique	45
13.	Gestion des clés	47
13.1.	En chiffrement symétrique	47
13.2.	En chiffrement asymétrique	48
13.2.1.	Infrastructures de clés publiques - PKI.....	48
13.2.2.	Les certificats.....	48
13.2.2.1.	But.....	48
13.2.2.2.	Principales caractéristiques des certificats	48
13.2.3.	Utilisation des certificats de clés publiques.....	49
13.2.3.1.	Création du certificat.....	49
13.2.3.2.	Distribution des certificats	49
13.2.3.3.	Validation des certificats.....	49
13.2.3.4.	Révocation et suspension des certificats	50
13.2.3.5.	Expiration et renouvellement	50
13.2.4.	Utilité des certificats de clés publiques	50
13.2.5.	Définition d'une ICP (Infrastructure de Clés Publiques)	50
13.2.6.	Politiques de certificats des ICP	51
13.2.7.	Acteurs d'une Infrastructure de clés publiques	51
13.2.7.1.	Autorité de certification (AC)	51
13.2.7.2.	Autorité d'enregistrement (AE)	51
13.2.7.3.	Bureaux d'enregistrement « métier », agence bancaire, direction des ressources humaines ou autres autorités compétentes.....	52
13.2.7.4.	Autorité de création de politique (ACP)	52
13.2.7.5.	Autorité d'approbation des politiques (AAP)	52
13.2.7.6.	Autorité d'horodatage (AH).....	53
13.2.7.7.	Autorité d'attributs (AA).....	53
13.2.8.	Modèles de confiance des PKI	53
13.2.8.1.	Architecture hiérarchique.....	53
13.2.8.2.	Architecture à base de certification croisée.....	54
13.2.8.3.	Architecture à base de point focal	54
14.	Parade contre les menaces	54
15.	Architecture sécurisée	55
15.1.	Considérations techniques d'une architecture de sécurité	55
15.2.	Mise en place d'une architecture sécurisée	55

15.2.1.	Routeur	56
15.2.2.	Filtrage IP	56
15.2.3.	Types de pare-feux	56
15.2.3.1.	Filtrage IP – pare-feux sans état	57
15.2.3.2.	Filtrage IP	57
15.2.3.3.	Règle de configuration de sécurité 1 avec le routeur R0	57
15.2.3.4.	Règles de configuration de sécurité 2 avec les routeurs R1 et R2	58
15.2.3.5.	Règle de configuration de sécurité 3(avec une zone DMZ ou démilitarisée) .	61
15.2.4.	Zone démilitarisée (DMZ)	61
15.2.5.	Gestion des services	62
15.2.6.	Proxy	62
15.2.7.	Masquerading (NAT)	63
15.2.7.1.	Objectifs et la raison d’être d’un NAT	63
15.2.7.2.	Types de NAT	63
16.	VPN (Virtual Path Network)	65
17.	Que faire après une attaque ?	66
18.	Normes ISO pour la SSI (Sécurité des Systèmes d’Information)	66
19.	Arsenal législatif	66
19.1.	Acteurs institutionnels en France	67
19.2.	Au niveau international	68
20.	Ingénieur sécurité : c'est un métier !	68
CONCLUSION		68
CHAPITRE III : WINDOWS ET LA CONFIGURATION DE LA SECURITE		70
INTRODUCTION		71
1.	Présentation	71
1.1.	Historique	71
1.2.	Les différentes versions de Windows	71
2.	Configuration des outils de sécurité Windows	72
2.1.	La configuration du pare feu (Firewall) pour la sécurité	72
2.2.	Gestion des comptes d'utilisateurs	75
CONCLUSION		78
CONCLUSION GENERALE		79
QUESTIONNAIRE AUX CHOIX MULTIPLES (QCM)		80
REPONSES AU QUESTIONNAIRE		83

RECUEIL DES EXERCICES	84
CORRIGES PROPOSES DES EXERCICES	91
TABLEAU DES COMMANDES SYSTEMES	98
COMMANDES MS-DOS	103
COMMANDES RESEAUX	107
GLOSSAIRE	109
BIBLIOGRAPHIE	135

