

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre De Recherche Sur L'information
Scientifique Et Technique



Mémoire de Projet de Fin D'études

En Vue de l'Obtention du Diplôme de post graduation spécialisé en Informatique

Option : sécurité informatique

Thème :

LE DARKNET UN SYSTÈME DE MONITORING POUR LA CYBER-SÉCURITÉ

Encadré par :

Encadreur : Melle. ZEGHACHE Linda
Co-encadreur : Mr. AMIRA Abdelouahab

Réalisé par :

Mr ATTOUI Lakhdar
Mr CHELOUACHE Abdellah

Devant le jury composé de :

Mme BENMEZIANE Souad
Mr Hadjar Samir
Mme GUEMRAOUI Leila

Présidente
Examineur
Examineur

Promotion 2017-2018

TABLE DES MATIERES

Table des matières

Liste des Abréviations	ix
Liste des Figures	xi
Liste des Tableaux.....	xiv
Introduction Générale	1
Chapitre 1 : la sécurité informatique	3
1.1 Introduction	3
1.2 Définition de la sécurité informatique	3
1.3 Évaluation de la sécurité d'un réseau	3
1.4 Les différents types d'attaques	4
1.4.1 Anatomie d'une attaque	4
1.4.2 Les attaque réseaux	5
1.4.3 Les attaques applicatives	9
1.4.4 Le Déni de service	10
1.4.5 Les virus	12
1.4.6 Les chevaux de Troie	13
1.4.7 Ingénierie sociale	13
1.5 Les moyens de sécurisé un réseau	13
1.5.1 Les Antivirus	13
1.5.2 Les mises à jour système	14
1.5.3 Les firewalls	14
1.5.4 Les architecture DMZ	15
1.5.5 Les VPN	16
1.5.6 Les IDS	17

1.5.7 Les IPS	17
1.5.8 La Sensibilisation du personnel	18
1.5.9 Audits de sécurité	18
1.5.10 Contrôle d'accès	18
1.5.11 Les protocoles de sécurité	19
1.5.12 Les Algorithmes de chiffrements	20
1.5.13 Les Systèmes de surveillance de la cyber-sécurité	20
1.6 Mise en œuvre d'une politique de sécurité	21
1.7 Conclusion	22

Chapitre 2 : Surveillance de la sécurité du cyber-espace 23

2.1 Introduction	23
2.2 Systèmes de surveillance de la cyber-sécurité reposant sur des pièges	23
2.3 Cyber-menaces détecté grâce les systèmes basés sur des pièges	24
2.4 Systèmes de surveillance du cyber-sécurité	26
2.4.1 Darknet	26
2.4.1.1 Déploiement de darknet	26
2.4.1.2 Données darknet	27
2.4.1.3 Darknet : Avantages et inconvénients	28
2.4.2 IP Gray Space	29
2.4.2.1 Déploiement IP Gray Space	29
2.4.2.2 Données IP Gray Space	30
2.4.2.3 IP Gray Space : Avantages et inconvénients	30
2.4.3 Honeypot	30
2.4.3.1 Déploiement de Honeypot	31
2.4.3.2 Données Honeypot	31
2.4.3.3 Honeypot : Avantages et inconvénients	32

2.4.4 Greynet	32
2.4.4.1 Déploiement de Greynet	32
2.4.4.2 Données Greynet	33
2.4.4.3 Greynet : Avantages et inconvénients	33
2.4.5 Honeytokens	33
2.4.5.1 Déploiement de Honeytokens	34
2.4.5.2 Données Honeytokens	34
2.4.5.3 Honeytokens : Avantages et inconvénients	34
2.5 Etude comparative	35
2.5.1 Comparaison des fonctionnalités	35
2.5.2 Distribution d'espace d'adresses	37
2.6 Etude de cas	38
2.6.1 Étude de cas basée sur darknet	38
2.6.2 Étude de cas basée sur un Honeypot	40
2.7 Politiques de sécurité et questions juridiques	41
2.7.1 La lutte contre la cybercriminalité en Algérie	41
2.7.2 Nuire aux autres	44
2.8 Conclusion	44
Chapitre 3 : Darknet en tant que source de cyber-sécurité	46
3.1 Introduction	46
3.2 Définitions de darknet	46
3.3 Fonctionnement de darknet	47
3.3.1 Les activités de scannage	47
3.3.2 Les 'attaques DDoS	48
3.3.3 Les 'attaques DRDoS	48
3.4 Données darknet	49

3.4.1	Techniques de traitement des données	50
3.4.2	Analyse de données darknet	51
3.4.3	Événements darknet globaux et locaux	52
3.5	La visibilité de darknet	53
3.5.1	Techniques de placement du capteur darknet.....	53
3.5.2	Configuration du Réseau darknet	54
3.6	Déploiement darknet	57
3.6.1	Techniques de déploiement	57
3.6.2	Provisionnement des ressources	59
3.6.3	Variantes darknet	61
3.7	Projets de surveillance du réseau darknet	62
3.7.1	Les projets de surveillance à grande échelle	62
3.7.2	Les projets de surveillance à moyenne échelle	66
3.7.3	Les projets de surveillance non classé	67
3.8	Visualisation darknet	68
3.9	Conclusion	69
Chapitre 4	La mise en œuvre du réseau darknet	70
4.1	Introduction	70
4.2	L'objectifs de la solution proposée	70
4.3	Schéma de l'architecture du réseau darknet	70
4.4	Choix de technique de déploiement	71
4.5	La mise en œuvre du réseau darknet	71
4.6	Les outils de déploiement	71
4.6.1	GNS3 (Graphical network simulator).....	71
4.6.2	VMware Workstation	72
4.6.3	L'application Nmap	72

4.6.4 File zilla client	72
4.6.5 Wireshark	73
4.6.6 Tcpdump	73
4.7 Configuration et lancement du réseau darknet	73
4.7.1 Les différents segments du réseau darknet	74
4.7.2 Les machines virtuelles	75
4.7.3 Configuration de réseau LAN	75
4.7.4 Configuration de la machine firewall avec deux interfaces	76
4.7.5 Configuration les deux routeurs R1 et ISP	78
4.7.6 Configuration de la machine VMware Server Darknet	81
4.7.7 Configuration de la machine VMware Kali linux	82
4.8 Test et validation	83
4.8.1 Collecte des données et stocké les paquets capturé	83
4.8.2 L'analyse des paquets capturé	85
4.8.3 Les statistiques des paquets capturé	87
4.9 Conclusion	90
5 Conclusion générale	91
6 Bibliographie	94
7 Annexe A	104