Enseignements de la CyberSécurité en DUT R&T

Chantal LABAT, Fabrice PEYRARD
IUT Blagnac, Dpt Réseaux & Télécoms, UT2J
Université de Toulouse, France
Email : {*Prenom.Nom*}@univ-tlse2.fr

***Résumé* — Le département R&T de l'IUT de Blagnac propose d'accentuer les enseignements en CyberSécurité au travers des modules du programme pédagogique national de 2013. Ces enseignements visent à sensibiliser les nouveaux bacheliers au vocabulaire et au monde numérique qui les entoure. Ils approfondiront les connaissances théoriques mais surtout pratiques dans les modules réseaux, systèmes et sécurité. Les modules informatiques pourront s'approprier le langage Python pour l'appliquer aux environnements de la CyberSécurité. Une grande importance sera accordée pour développer un comportement de hacker éthique.**

Mots-clés* — *CyberSécurité, Hack Ethique, Réseaux, Pentesting, Linux, Logs, ANSSI

I. INTRODUCTION

Dans un contexte grandissant des cyber-menaces les enseignements en CyberSécurité nécessitent d'être clairement identifiés dans la formation du DUT R&T afin de sensibiliser, d'initier et d'apprendre les règles de bon usage des réseaux et des systèmes d'informations. L'objectif de cet article est de présenter une façon d'aborder les enseignements de CyberSécurité en DUT Réseaux & Télécoms pour former les étudiants à la pratique des bonnes règles d'usage et à les initier à des concepts techniques avancés de CyberSécurité pour ceux qui souhaiterons poursuivre leur formation spécialisée dans ce domaine.
Dans l'objectif de dynamiser la communauté DUT Réseaux & Télécoms aux enseignements de la CyberSécurité, le WiKi CyberRT [1] a été mis en place à cet effet.
L'ensemble des ressources liées à cet article sont disponibles ici [2].

II. SENSIBILISATION A LA CYBERSECURITE

A. Contexte

Pour former les étudiants à la CyberSécurité, il est nécessaire, dans un premier temps de les sensibiliser et de leur expliquer les rudiments élémentaires de la sécurité ainsi que les techniques et les réflexes pour les mettre en application. Généralement les lycées des BAC généraux S et techniques STI2D sont très rarement sensibilisés aux problématiques de la CyberSécurité. Il s'agit, dès la première année du DUT R&T, dans les modules d'initiation aux réseaux, informatique et systèmes de sensibiliser les étudiants aux menaces des cybercriminels.

Il est indispensable de définir le nouveau vocabulaire afin d'agréger peu à peu les compétences pour que, in fine, à l'issue de deux ans de formation, les diplômés du DUT R&T soient capables d'appliquer des procédures de CyberSécurité.

B. Bonnes pratiques en matière de sécurité du SI

L'objectif est de connaître les documents relatifs à la mise en œuvre des bonnes pratiques en matière de sécurité du SI [26] comme, par exemple le guide d'hygiène informatique de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
Il sera demandé aux étudiants de travailler sur les préconisations proposées par ce guide.
Par exemple pour la sensibilisation à la CyberSécurité on s'appuiera sur la mesure n°7 « Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés ». Les étudiants devront interpréter la recommandation en proposant un schéma de l'architecture réseau avec l'implantation des points d'accès WiFi, la définition des différents SSID et la proposition d'une solution d'authentification 802.1x.
Dans un contexte de sécurité avancée, on peut mener une réflexion avec les étudiants sur l'application de la mesure n°17 : « Activer et configurer le pare-feu local des postes de travail ».

Les étudiants devront vérifier les applications utilisant les ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix pour en déduire des vulnérabilités potentielles exploitées par le ransomware `WannaCry` en s'aidant par exemple des sites de `Snort` [27] et `Talos` [28].

C. Définition et vocabulaire

Tout commence par les définitions des hackers dont on distingue 3 catégories :

Les chapeaux blancs (white hat) : il s'agit de pirates éthiques qui utilisent leurs compétences en matière de programmation à des fins bénéfiques, éthiques et légales. Les hackers en chapeau blanc peuvent effectuer des tests de pénétration du réseau en utilisant leurs connaissances des systèmes de sécurité informatique pour compromettre les réseaux et les systèmes afin de découvrir les différentes vulnérabilités.

Les chapeaux gris (gray hat) : il s'agit de personnes qui commettent des délits et dont l'éthique est discutable, mais qui ne le font pas pour leur gain personnel ou pour causer des dommages. Ce peut être, par exemple une personne qui compromet un réseau sans autorisation, puis dévoile publiquement la vulnérabilité.

Les chapeaux noirs (black hat) : il s'agit de criminels malhonnêtes qui enfreignent la sécurité des ordinateurs et des réseaux pour leur gain personnel ou à des fins malveillantes. Les hackers en chapeau noir exploitent les vulnérabilités afin de compromettre les systèmes informatiques et les réseaux.

Il est important de comprendre que parmi ces hackers, certain sont identifiés comme des « script kiddies » ou hackers inexpérimentés qui exécutent de petits programmes ou scripts sans savoir exactement l'étendue de leurs actions. Les plus dangereux sont les cyber-criminels qui travaillent à leur compte ou pour de grandes organisations mafieuses dont les transactions ont lieu dans le Darknet utilisant des crypto-monnaies. A titre d'exemple, le 28 juin 2018, Europol [3] a démantelé un réseau de producteurs et vendeurs de drogues de type LSD sur le Darknet et dont 4.5 millions d'euros en bitcoin ont été saisis. Le cyber-espace s'avère un microcosme extrêmement complexe dont les attaques peuvent être liées aux réseaux, systèmes, données, … et dont leurs vocations ont pour seul but d'être criminelles.

D. Créer un monde numérique

Appréhender le monde de la CyberSécurité par la pédagogie inversée est une approche innovante. Sans connaître les principes fondamentaux des réseaux et des protocoles IP, TCP et UDP, il est intéressant d'inculquer les concepts de sécurité dans le module « Initiation aux réseaux d'entreprise » en s'appuyant sur les Labs « Créer un monde numérique » [4] et « Communiquer dans un monde numérique » [5]. En effet, ce module permet d'illustrer une topologie de réseaux interconnectés au travers d'Internet en mettant en évidence les principaux éléments actifs (switch, routeur, point d'accès, modem DSL) ainsi que les principaux services Web, FTP, DNS, Messagerie, NTP, AAA. Cela permettra de donner les premières définitions de la confidentialité, intégrité et disponibilité.

E. Menaces, vulnérabilité et attaques

Au-delà des infrastructures matérielles, il s'agit de donner la définition de malware et de ses différentes formes (virus, vers, chevaux de Troie) et surtout d'insister sur celles de type Ransomware [6] au travers d'attaques utilisant des failles ou des techniques de fishing par le mail. Il s'agira de sensibiliser fortement les jeunes aux mécanismes de l'ingénierie sociale au travers des emails, SMS et réseaux sociaux.

Dans le module « Technologie de l'Internet », lorsque les étudiants ont suffisamment de connaissances en système Linux, éléments actifs et protocoles IP, il est alors intéressant de leur faire manipuler [7] des outils de détection des menaces et des vulnérabilités comme `nmap` [8] par exemple qui permet d'identifier les ports ouverts d'un système et être utile en affichant les versions des systèmes pour rechercher les vulnérabilités potentielles.

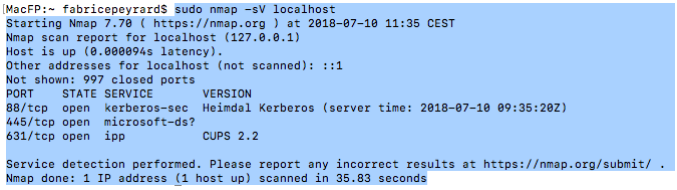


Fig. 1. Utilisation locale de `nmap`

Il est souhaitable de compléter cette première approche de `nmap` par une utilisation avancée [12] pour le scan d'équipements distants où on pourra déceler, par exemple, les ports ouverts sur le routeur de sortie (default gateway) grâce à l'outil graphique `Zenmap` [9].

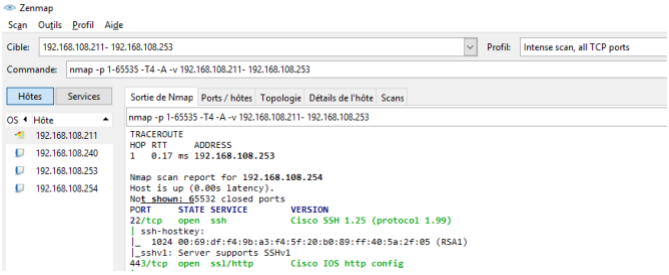


Fig. 2. Utilisation de `Zenmap`

En semestre 3, dans le module « Services réseaux avancés », dont les enseignements se font généralement dans l'environnement Linux, il est important de comprendre la notion de « renforcer un système Linux » [11], ou durcissement. L'outil `lynis` [10] permet de faire un audit d'un système Linux et de proposer des recommandations pour renforcer sa sécurité. On aperçoit fréquemment des remontées d'alertes faisant référence à des services usuels insuffisamment sécurisés.

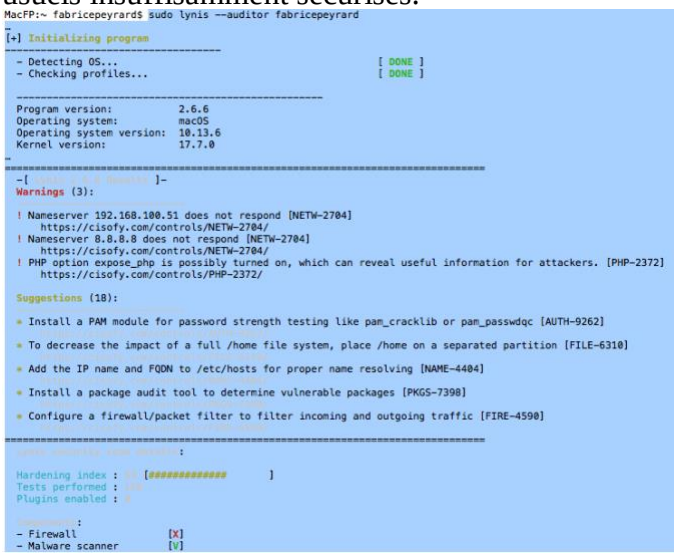


Fig. 3. Utilisation de `lynis`

Dans le contexte d'étude des vulnérabilités, les nombreuses failles des sites Internet sont examinées. Elles sont souvent un moyen de pénétrer dans le système d'information dû à des niveaux insuffisant de sécurité d'authentification des utilisations et des modules supplémentaires non mis à jour. Parmi les outils de détection de vulnérabilités des serveurs Web, on peut citer `Netsparker` [33]. Cet outil permet rapidement de connaitre les degrés de vulnérabilité des failles, comme par exemple ici seule la version TLSv1 supportée.

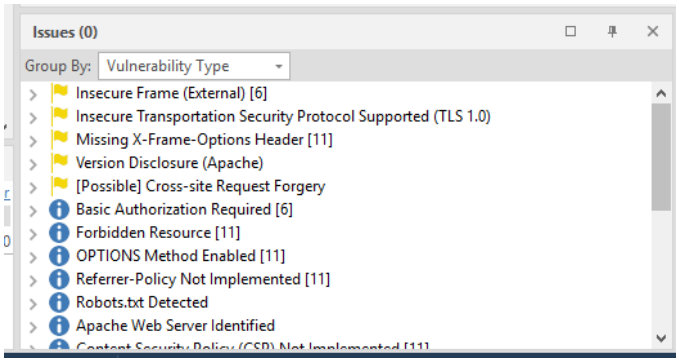


Fig. 4. Exemple d'une vulnérabilité de faible niveau TLS

III. Enseignements specialises a la CyberSecurite

A. *Confidentialité*

Dans une approche plus spécifique de la CyberSécurité en DUT R&T, en particulier dans les modules complémentaires « Sécurité et performance » et « Sécurisation des services réseaux », il sera nécessaire d'introduire les mécanismes généraux de chiffrement symétrique et asymétrique. Afin d'appréhender cette problématique de la confidentialité des données stockées localement et transmises via le réseau, un cas d'usage peut être, l'utilisation des signatures numériques [13] en s'appuyant sur l'algorithme RSA [14] et sur un outil de chiffrement en ligne [15].

En s'appuyant sur la même topologie précédente de réseaux et de services (II.D), il est intéressant de comprendre comment explorer le contenu de fichiers chiffrés [16], d'utiliser des outils [17] en ligne pour déchiffrer et accéder à des services réseaux dont les données d'authentification (login/motdepasse) étaient chiffrées au préalable.

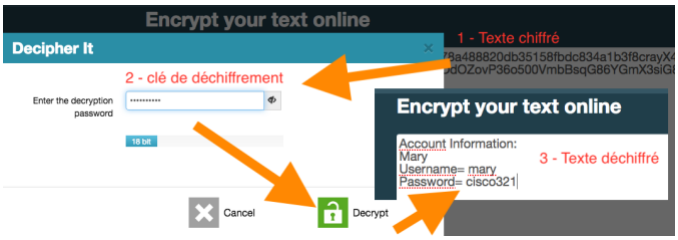


Fig. 5. Déchiffrement AES-256

B. *Intégrité*

L'intégrité des données fait partie des notions fondamentales de la sécurité en particulier pour s'assurer que des données n'aient pas pu être altérées ou corrompues lors d'un transfert de fichiers. Le téléchargement d'applications complémentaires sur un système d'exploitation doit aujourd'hui, nécessairement être accompagné d'une vérification de l'intégrité des données reçues. Pour cela une application de génération d'empreintes est effectuée sur fichiers à partir des algorithmes de hachage MD5, SHA1 et SHA2 implémentés dans OpenSSL [18].

En s'appuyant également sur la topologie précédente de réseaux et de services (II.D), il est intéressant de comprendre la nécessité de vérifier l'intégrité des fichiers au travers de leurs empreintes. Le hash en clair [20] ou chiffré (HMAC) [21] peut être obtenu avec des outils en ligne.

C. *Attaque par dictionnaire*

La complexité des mots de passe est une des règles d'hygiène informatique fortement préconisée par l'ANSSI pour sécuriser les postes de travails, serveurs, éléments actifs, … Une des principales méthodes pour trouver les mots de passe des comptes utilisateurs est une attaque par dictionnaire [23]. La distribution Linux Kali [24] ou bien BlackArch [25] intègre nativement de multiples outils liés au pentesting et au hacking éthique, dont « John the Ripper password cracker » [32].

Dans un contexte d'entreprise, ce genre de procédure peut être réalisée sur le système d'information en cas d'oubli de mot de passe de la part d'un utilisateur ou bien pour d'autres raisons mais ayant un enjeu « vital » de l'entreprise.

Fig. 6. Attaque par dictionnaire

Il est important de préciser aux jeunes en apprentissage, que ces enseignements de CyberSécurité, et l'ensemble des outils présenté sont exclusivement voués à être utilisé dans un contexte éthique. On parle alors de « Ethical Hacker » ou bien de « White Hat ».

D. *Outils de Pentesting*

Il est souvent utile de pouvoir « forger » ses propres trames Ethernet, paquets IP, entêtes TCP, UDP, … Parmi les nombreux outils, citons `Scapy` [22] qui initialement permet de découvrir les équipements du réseau, de scanner des ports, de tracer les routeurs, … et qui peut être également utilisé pour générer des paquets dans l'objectif de tester les sondes d'intrusion réseau (Intrusion Detection System). On peut facilement forger un paquet de requête DNS à partir de la primitive `sendp` suivante.

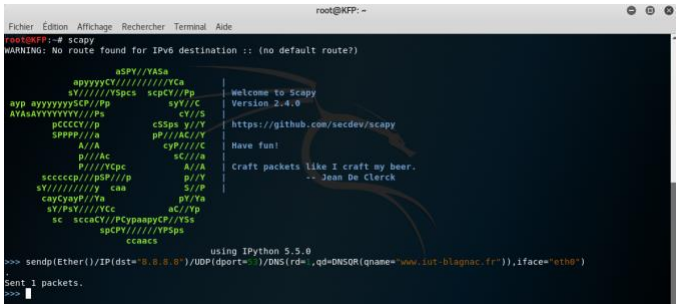


Fig. 7. Requête UDP forgée avec Scapy

On n'oubliera pas de vérifier l'émission correcte de la trame avec le « couteau suisse des R&T », à savoir Wireshark.

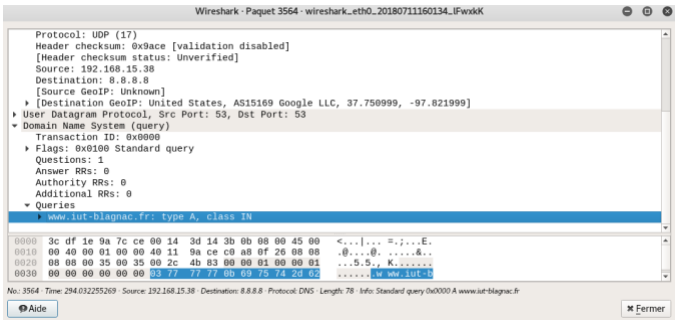


Fig. 8. Analyse avec Wireshark de la requête UDP forgée

IV. Architecture sécurisée VPN IPSec / SSL

L'objectif de cette partie est de sécuriser l'interconnexion de réseaux vu en section (II.D) par la mise en œuvre de tunnels VPN. Il s'agit dans un premier temps de configurer un tunnel IPSec entre un routeur Cisco et un ASA 5505 à partir du Lab CCNA Security [30].

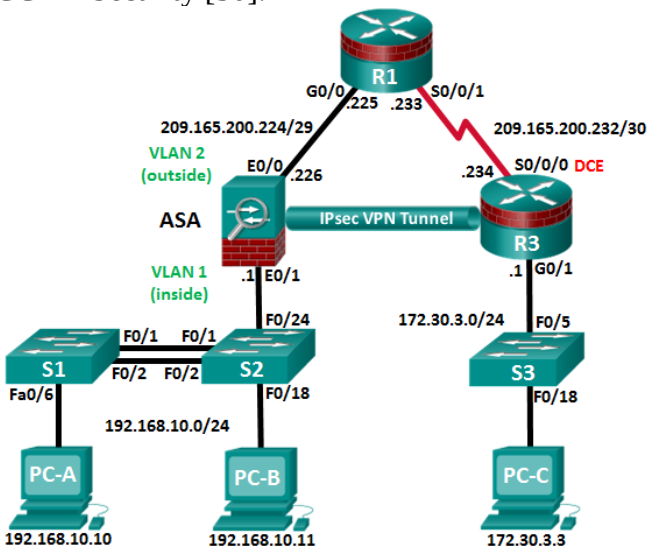
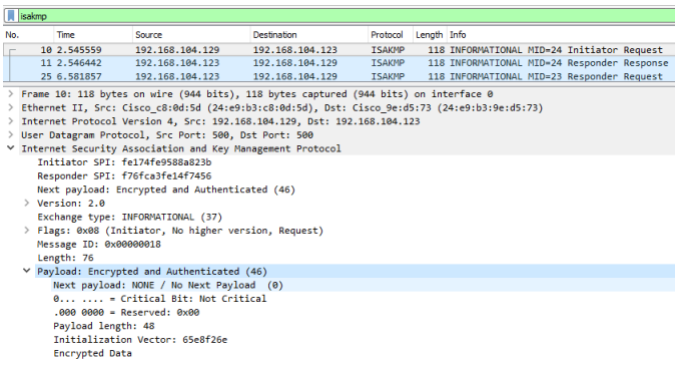


Fig. 9. Architecture sécurisée VPN

Au-delà des spécificités de configuration, on s'attachera à l'analyse des protocoles ISAKMP et ESP du tunnel IPSec.



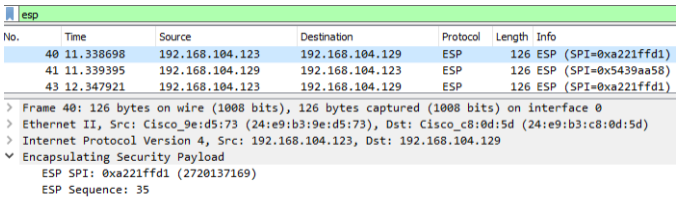


Fig. 10. Analyse avec Wireshark des protocoles ISAKMP et ESP

Puis dans un deuxième temps, en s'appuyant sur un Lab similaire [31], il faudra paramétrer un client nomade et sa connexion VPN/SSL pour qu'il puisse accéder aux ressources entreprises localisées après le firewall ASA.

V. Surveillance de la Securite du Reseau

La surveillance du réseau appelé aussi NSM (Network Security Monitoring) peut être implémentée avec différents outils incluant les sondes de détections réseau (IDS), les analyseurs de protocoles, l'utilisation du protocole de supervision SNMP et les journaux de log du SI et des éléments actifs.

A. Pourquoi les logs ?

Depuis plus de 30 ans, les systèmes d'information et les éléments actifs du réseau sont conçus pour générer des journaux d'évènements appelés « log » permettant de conserver un historique des comportements normaux ou anormaux de ces systèmes. Pendant de nombreuses années, ces journaux étaient souvent explorés manuellement après l'observation d'un évènement anormal. Ce travail de gestion des logs est à la charge de l'administrateur système et/ou réseau. Aujourd'hui, le constat est différent, car les « logs » sont la source de remontées d'alertes et surtout la corrélation des logs entre eux pour permettre de déceler des vulnérabilités potentielles de l'ensemble du système mais également des attaques ciblées ou distribuées.

L'apprentissage de la CyberSécurité doit nécessairement passer par la connaissance des logs et des outils logiciels pour les collecter et les traiter.

B. Localisation des fichiers de logs

Pour comprendre le mécanisme de journalisation des évènements systèmes, en s'appuyant sur une distribution Linux, on s'intéressera à la localisation des fichiers [34] en particulier ceux dans le répertoire `/var/log`. A titre d'illustration on

observera également les logs générés en temps réel par l'application du serveur Web `nginx` et la commande de traitement des journaux `journalctl` [35].

C. Suivi des logs du réseau

Les éléments actifs d'un réseau (switch, routeur, firewall, …) sont source de nombreux logs générés, provenant soit intrinsèquement du système d'exploitation (IOS) soit par la nature des paquets y transitant. Généralement les éléments actifs ne disposent pas de capacité suffisante pour stocker et archiver les logs, il est donc commun de les rediriger avec un système `syslog` [36] [37].

A titre d'exemple, il est intéressant d'observer en temps réel le changement d'état d'une carte réseau d'un système Linux lors de l'utilisation de la commande `Scapy` pour forger un paquet.

Fig. 11. Syslog en temps réel – impact de `Scapy`

Lorsque le paquet forgé par Scapy est envoyé sur l'interface réseau (`eth0`) cette dernière commute en mode `promiscuous` le temps de l'émission, ce qui lui permet d'accepter tous les paquets qu'elle reçoit.

L'étude, la corrélation des logs et les outils associés sont indispensables pour appréhender le nouveau métier « analyste sécurité » notamment au sein d'un un SOC (Security Operations Center).

VI. CONCLUSION

Durant ces vingt dernières années, la sécurité des systèmes d'information et des réseaux a fait émerger le domaine de la CyberSécurité, en particulier à cause de l'exposition des moyens de transmission réseau et des systèmes de plus en plus virtualisés. La formation en DUT Réseaux & Télécoms a toujours pris en compte, dans les enseignements, cette approche de la sécurité. Cependant il est indispensable aujourd'hui d'intégrer dans la formation, des enseignements de CyberSécurité. Nous avons présenté dans cet article, une façon d'introduire la CyberSécurité dans les enseignements réseaux et systèmes. Cette approche vise à parcourir le domaine de la CyberSécurité, de la sensibilisation jusqu'aux approches techniques spécifiques de pentesting dans un contexte de hack éthique.

Références

[1] https://goo.gl/jra64E
[2] https://goo.gl/Q2q7oJ
[3] Police seize more than EUR 4.5 million in cryptocurrencies in Europe's biggest ever LSD bust https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe%E2%80%99s-biggest-ever-lsd-bust
[4] Lab Creating a Cyber World – Netacad Cisco CyberEssential 1.5.3.5
[5] Lab Communicating in a Cyber World – Netacad Cisco CyberEssential 1.5.3.6
[6] Ransomware - Anatomy of an Attack https://youtu.be/4gR562GW7TI
[7] Lab - Detecting Threats and Vulnerabilities – Netacad Cisco CyberEssential 3.3.1.9
[8] https://nmap.org/
[9] https://nmap.org/zenmap/
[10] https://cisofy.com/lynis/
[11] Lab Hardening a Linux System – Netacad Cisco CyberEssential 7.1.1.6
[12] Lab Exploring Nmap – Netacad Cisco CyberOps 4.5.2.10
[13] Lab Using Digital Signatures – Netacad Cisco CyberEssential 5.2.2.4
[14] https://fr.wikipedia.org/wiki/Chiffrement_RSA
[15] http://nmichaels.org/rsa.py
[16] Lab Exploring File and Data Encryption – Netacad Cisco CyberEssential 2.5.2.6
[17] https://encipher.it/
[18] Lab Hashing Things Out – Netacad Cisco CyberOps 9.1.2.5
[19] Lab Using File and Data Integrity Checks – Netacad Cisco CyberEssential 2.5.2.7
[20] https://www.tools4noobs.com/online_tools/hash/
[21] https://www.freeformatter.com/hmac-generator.html
[22] https://scapy.net/
[23] Lab Password Cracking – Netacad Cisco CyberEssential 5.1.2.4
[24] https://www.kali.org/
[25] https://blackarch.org/
[26] https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
[27] https://blog.snort.org
[28] https://www.talosintelligence.com/
[29] https://www.ssi.gouv.fr/guide/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-a-internet/
[30] Lab CCNASv2_SKillsAssessment-B_Student_Training – Netacad Cisco Security
[31] Lab CCNASv2_SKillsAssessment-A_Student_Training – Netacad Cisco Security
[32] http://www.openwall.com/john/
[33] https://www.netsparker.com/
[34] Lab Locating Log Files – Netacad Cisco CyberOps 3.2.1.4
[35] Lab Reading Server Logs – Netacad Cisco CyberOps 7.3.2.5
[36] Lab Logging Network Activity – Netacad Cisco CyberOps 7.1.2.7
[37] Lab Logging from Multiple Sources Instructions – Netacad Cisco CyberOps 11.2.3.11