

SEC102

Menaces informatiques et code malveillants : analyse et lutte

Parcours :

- CC13800A : Certificat de compétence Analyste en cybersécurité
- CPN8401A : Architecte infrastructure Réseaux et systèmes
- CPN8402A : Chef de projet maîtrise d'œuvre informatique
- CPN8403A : Architecte en Cybersécurité
- LG02501A : Licence générale Sciences technologies santé mention informatique parcours Informatique générale

Parcours :

- CYC9101A : Diplôme d'ingénieur Spécialité informatique parcours Architecture et ingénierie des systèmes et des logiciels (AISL)
- CYC9102A : Diplôme d'ingénieur Spécialité informatique parcours Informatique modélisation optimisation
- CYC9104A : Diplôme d'ingénieur Spécialité informatique parcours Informatique, réseaux, systèmes et multimédia
- CYC9105A : Ingénieur informatique système d'information et business intelligence
- CYC9106A : Diplôme d'ingénieur Spécialité informatique parcours Cybersécurité

Objectif

- Comprendre les modes d'action pour prévoir les effets (**phase de veille**)
- Détecter les effets des codes malveillants (**phase d'alerte**)
- Minimiser, stopper ou réduire l'impact du code malveillant (**phase de réponse**)

VEILLE

Stratégie de Cyberdéfense & SECOPS dans le maintien en condition de sécurité

REPONSE

DEFENDRE LES ACTIFS

ALERTE

Identifier son
écosystème
digital

Remédier et
reconfigurer
pour limiter
l'impact

Repérer et suivre
ses
fragilités

Surveiller
les
sources de
menaces

Détecter
des attaques
dans les
événements

Alerter en
fonction de
l'impact

Enquêter sur
l'incident

Identifier,
caractériser
les
menaces

S'entraîner

Neutraliser
les sources
de menaces

PROTEGER SES ESSENTIELS

MAINTENIR LA CONTINUITE D'ACTIVITE

© EDU 2017 - Orange Cyberdefense LIOVAR Model

SEC102

Menaces informatiques et codes malveillants : analyse et lutte

le **cham**
CyberSécurité

Présentation de l'intervenant

Je suis Thierry Veyre. Mon adresse de messagerie est « thierry.veyre@lecnam.net ». Je suis consultant en cyber sécurité, inventeur ou co inventeur de 12 brevets dans les domaines de la résilience de système d'information

1998 – 2015, **SERVICES2I**, fondateur associé, président

Depuis 2014, **SUNBREN**, inventeur associé, responsable du laboratoire de recherche

Depuis 2015, **ISIE**, fondateur associé, consultant en cyber sécurité

Depuis 2018, **SERENICITY**, inventeur associé, responsable du laboratoire de recherche

Depuis 2018, **EXPERT PRES LA COUR D'APPEL DE LYON**, domaines d'expertise E.01.03 (logiciels et matériels) et E.01.04 (mise en œuvre systèmes d'information)

Depuis 2019, **EXPERT NUMERIQUE DCPJ**, collaboration avec la division D2A (division de l'anticipation et de l'analyse) de la Direction Centrale de la Police Judiciaire à Nanterre

Depuis 2019, **EXPERT NUMERIQUE C3N/COMCYBERGEND**, collaboration avec le C3N (centre de lutte contre les criminalités numériques) de la Gendarmerie Nationale et le COMCyberGEND (commandement de la gendarmerie dans le cyberspace) à Cergy-Pontoise

Depuis 2020, **CNAM**, enseignant en charge des cours SEC102 pour la région AURA et SEC106 FOAD pour Paris

Introduction

- A. Qualité technique et rédactionnelle
- B. Avant propos
- C. Rappels
- D. Introduction aux fonctions cryptographiques

Qualité technique et rédactionnelle

1. Le fond et la forme
2. Page de garde
3. Sommaire
4. Contexte
5. Langue, orthographe et grammaire
6. Conclusion du rapport
7. Version
8. Validation
9. Confidentialité
- 10. Format PDF (obligatoire)**

Qualité technique et rédactionnelle

Le fond et la forme

- Qualité technique
- Qualité rédactionnelle de la restitution technique
- La nécessité d'un rapport structuré

Qualité technique et rédactionnelle

Page de garde

- Identification de l'entreprise ou de l'organisme
- Titre
- Nommage et référence du document
- Auteur, date, version, validation et diffusion

Qualité technique et rédactionnelle

Contexte

- Objectifs
- Public visé.
- Pré requis
- Etat de l'art
- ...

Qualité technique et rédactionnelle

Langue, orthographe et grammaire

- Respect de l'orthographe
- Respect de la grammaire
- Respect de la ponctuation propre de la langue employée
- Bannir les expressions du langage courant
- Citer ses sources (respect du droit d'auteur)

Qualité technique et rédactionnelle

Conclusion du rapport

- Constats vis-à-vis des objectifs
- Extension du contexte

Qualité technique et rédactionnelle

Versions

- Tableau des versions
- Date(s)
- Auteur(s)
- Commentaire(s)

Qualité technique et rédactionnelle

Validation (facultatif pour les TP)

- Tableau des validations
- Création et modification
- Approbation
- Cycle de validation à plusieurs étapes
- Validation interne et externe

Qualité technique et rédactionnelle

Confidentialité (facultatif pour les TP)

- Filigrane
- Documents numériquement signés
- Données noires / grises / blanches
- Cybersécurité et confidentialité (cloud)

Qualité technique et rédactionnelle

Format PDF

- Systématiser l'utilisation du format PDF pour un rapport
- Dans la mesure du possible, signer numériquement le rapport

Avant propos

Positionnement des UE SEC101 et SEC102

- SEC101 pour la vision globale à 360° des risques cyber
- SEC102 pour la vision ciblée à 1° d'un risque cyber

Avant propos

Positionnement RSX112 et SEC102

- Durant RSX112, vous étudiez :
 - certaines routines, commandes, utilisation de fonctions (avantages / inconvénients)
 - Système de sécurisation (avantages / inconvénients)
- C'est à partir de ces avantages et inconvénients que nous allons voir :
 - Ce qui peut être intéressant d'utiliser pour un attaquant
 - Quels éléments l'attaquant aura envie de récupérer
- Ces alertes n'auront pas toutes la même importance.
- La détection de ces signaux nécessite la prise en compte de plusieurs facteurs :
 - La complexité du code malveillant (longueur, obfuscation,...)
 - Votre habitude à retrouver ces signaux
 -

Plan du cours

Introduction

Courte introduction aux fonctions cryptographiques

1. Typologies des codes et des effets
2. Études des modes action des codes malveillants
3. Lutte contre le code malveillant
4. Caractérisation des effets, impacts techniques, économiques, fonctionnels
5. Réduction des effets, limitation des impacts techniques et de fonctionnels
6. Analyse post-mortem (forensic)
7. Méthodologies de réponses à incidents
8. Audits
9. Sujet final

TP N°1 : Positionnement du cours dans l'environnement: Motivations et objectifs derrière les nuisances ?

Positionnement de SEC102 dans l'environnement économique:

Pourquoi des failles, quel sont les sens et les motivations des actes qui viennent nuire à la sécurité des systèmes.

- Les motivations ou les causes d'actes qui viennent nuire a fonctionnement des systèmes sont nombreuses.
- L'objectif est de faire une phase de reconnaissance de « l'adversaire » en énumérant 5 types de nuisance concrète, leurs motivations et leurs impacts

Format du livrable avec un exemple

Nom de la nuisance informatique	Type de nuisance	Motivations	Vecteur	Profits estimés	Coûts estimés	Références
NotPetya	Ransomware de chiffrement/effacement de donnée	Suspicion d'attaque économique (non démontrée)	Logiciel de comptabilité Me-Doc	Pas de source, a priori faible d'après les articles	10 Milliards de dollars - Des arrêts de productions, et des problèmes de stock	notpetya: su r medium.c om

Avant propos

Editeur de code préconisé pour l'UE et les TP à venir : Visual Studio ou Visual Studio Code

- <https://visualstudio.microsoft.com/fr/vs/getting-started/>
 - Choisir la version Community (vs_community.exe)
- <https://code.visualstudio.com/download>
- <https://docs.microsoft.com/fr-fr/visualstudio/install/create-an-offline-installation-of-visual-studio>

Pour visual studio

- ☐ Ouvrir une invite de commande en tant qu'administrateur
- ☐ Se positionner dans le répertoire de récupération du fichier vs_community.exe
- ☐ Lancer la commande suivante afin créer une source locale d'installation
- ☐ `vs_community.exe --layout c:\vslayout --lang fr-FR`

c:\vslayout étant le répertoire de récupération

Avant propos – Mise en place par l’auditeur

VM Windows

Pour réaliser les certains TP, vous aurez besoin de Windows.

Vous pouvez récupérer une image de Windows conseillée par l’intervenant

Dernière version de Windows avec logiciels complémentaires

- <https://developer.microsoft.com/fr-fr/windows/downloads/virtual-machines/>

Windows 10 sans logiciels complémentaires :

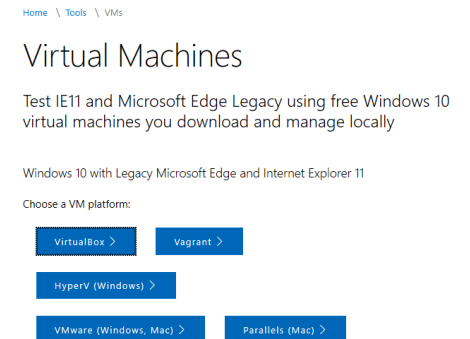
- <https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-10-enterprise>

Windows 11 sans logiciels complémentaires :

<https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-11-enterprise>

Vous pouvez récupérer VirtualBox + Extension Pack

- <https://www.virtualbox.org/wiki/Downloads>



A- Avant-propos – Logiciels à mettre sur la VM

- Téléchargez depuis votre VM
 - SysinternalsSuite <https://download.sysinternals.com/files/SysinternalsSuite.zip>
 - CFF Explorer <https://ntcore.com/files/ExplorerSuite.exe>
 - PE Studio <https://www.winitor.com/download>
 - Volatility (version 2.6 pour Windows 10) <https://www.volatilityfoundation.org/releases>
 - Volatility Workbench : <https://www.osforensics.com/tools/volatility-workbench.html>

Avant propos- Réglementation

Atteintes aux systèmes de traitement automatisé de données

Des crimes et délits contre les biens

- Accéder ou se maintenir
- Entraver ou fausser
- Introduire, modifier ou supprimer frauduleusement

Atteintes à la vie privée et au secret des correspondances

Interceptions des télécommunications

- Accomplie au vue et au sue des intéressés sans qu'ils s'y soient opposés
- Commis de mauvaise foi [...] procéder à l'installation conçus pour réaliser de telles interceptions

Préservation des traces et indices

Des atteintes à l'action de justice

- De modifier l'état des lieux d'un crime ou d'un délit [...] par l'altération, la falsification ou l'effacement des traces ou indices, soit par l'apport, le déplacement ou la suppression [...]
- De détruire, soustraire, receler ou altérer un document [...] de nature à faciliter la découverte d'un crime ou d'un délit [...]

Code Pénal

- Articles 323-1 à 323-3
- Articles 434-4
- Article 226-1 et 226-15



Avant propos – Rappels PSSI

Définition d'un système d'information

- Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs. Il s'agit d'un système socio-technique composé par:
 - Le sous-système technique est composé des technologies et des processus d'affaires concernés par le système d'information (ordinateur, système d'exploitation, logiciel, progiciel, routeur (box), borne sans fils, ...).
 - Le sous-système social est composé de la structure organisationnelle et des personnes liées au SI.

Avant propos – Rappels PSSI

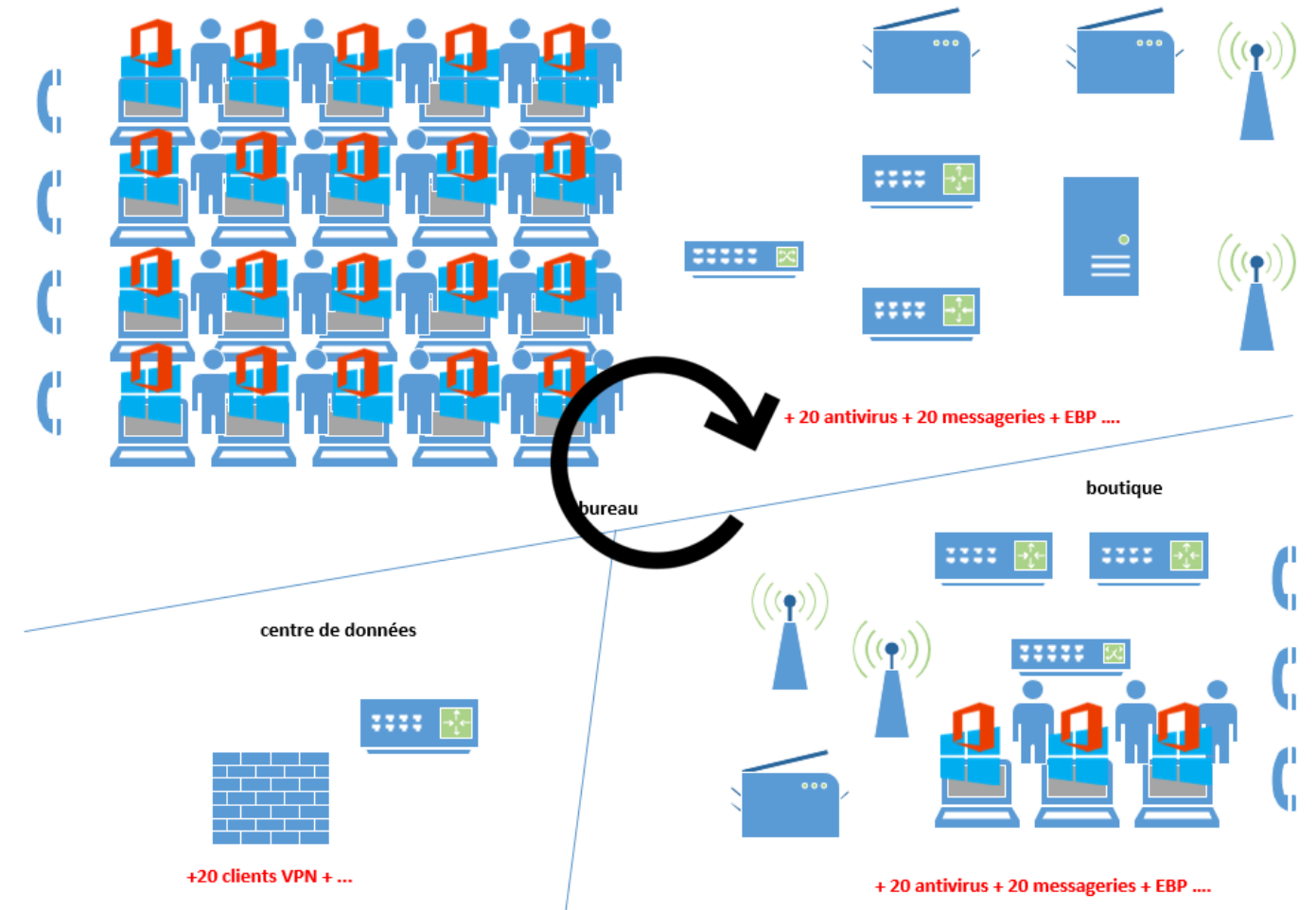
Un système d'information est une entité vivante...

- Mise à jour des systèmes d'exploitation
- Mise à jour des logiciels et progiciels
- Mise à jour des composants du réseau
- Arrivée et départ d'un collaborateur
- Gestion des tiers sensibles
- ...

... dans un éco système vivant

- Loi, décret, obligation légale, ...
- Cyber menaces
- RGPD
- ...

Avant propos – Rappels PSSI



Avant propos – Rappels PSSI

Politique de sécurité du système d'information

La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, État, unions d'États...) en matière de sécurité des systèmes d'information (SSI).

La PSSI constitue le principal document de référence en matière de SSI de l'organisme. Elle en est un élément fondateur définissant les objectifs à atteindre et les moyens accordés pour y parvenir.

Avant propos – Rappels PSSI

Politique de sécurité du système d'information

- Présentation de l'**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
 - L'ANSSI est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
- Présentation du guide d'hygiène informatique de l'ANSSI
 - Parmi les mesures techniques que les entités publiques ou privées doivent prendre pour garantir la sécurité de leurs systèmes d'information, on qualifie les plus simples et élémentaires d'entre elles d'hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.
 - 42 règles de BON SENS !

<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

Avant propos – Rappels PSSI

Politique de sécurité du système d'information

Le kit de survie MMS :

- Mot de passe (accent de la langue française)
- Mise à jour
- Sauvegarde (fonctionnelle et vérifiée)

Avant propos – Rappels PSSI

Politique de sécurité du système d'information

L'implication des collaborateurs dans la PSSI est indispensable:

- Charte utilisateur
- Sensibilisation
- Formation
- Recyclage des connaissances/compétences

Courte introduction aux fonctions cryptographiques

Rappels

Classification d'attaque

- **Attaque de reconnaissance**
 - Découverte écosystème (infrastructures, services, OS,...)
 - Pour obtenir les vulnérabilités exploitables
- **Attaque d'accès**
 - Attaque du réseau et/ou des systèmes
 - Pour accéder aux systèmes, obtenir des privilèges et/ou accéder aux données
- **Déni de service**
 - Attaque du réseau et/ou des systèmes
 - Pour empêcher l'usage
- **Cryptanalyse**
 - Attaquer les échanges
 - Porter atteinte à la confidentialité et/ou à l'intégrité des données

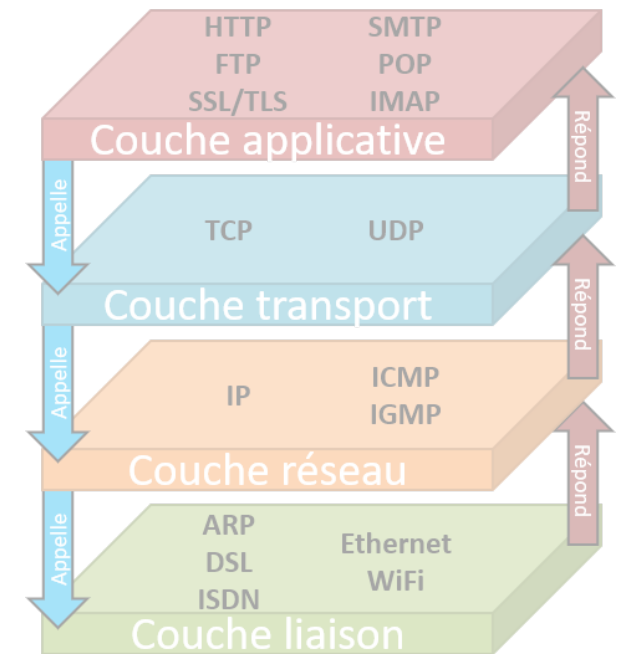
Rappels

Les vecteurs d'attaques

- Virus et Vers
- Les failles logicielles
 - Défaut de configuration
 - Zero Day
 - Bugs
 - Défaut de programmation / interprétation des commandes
- Les failles matérielles
- Les failles humaines
 - Ingénierie sociale

• Les failles ou détournement protocolaires

- ARP
- IP
- TCP
- UDP
- SMTP
- SNMP
- DNS
- FTP(S)
- HTTP(S)
- RDP



Positionnement de la problématique

Contexte – Positionnement de la problématique

La sécurisation d'un système est **l'ensemble des dispositifs** mis en œuvre afin de à la fois limiter et de garantir son usage aux utilisations légitimes.

La définition de la sécurisation d'un système est donc dépendante à la fois des caractéristiques du système en question et de son contexte.

- Première question : ***QUE CHERCHE-T-ON À « SÉCURISER » ?***
 - Information numérique
 - Communications sur un canal
 - Machines reliées par un réseau
 - Des échanges entre utilisateurs
 - Des processus métiers d'une organisation
 - ...

Positionnement de la problématique

Contexte – Les besoins/services de sécurité

Une solution technique avec une portée limitée : la cryptographie

Pour répondre à une définition fonctionnelle des besoins de sécurité il faudra combiner les techniques, méthodes et mesures de sécurité.

- **Confidentialité**
- **Intégrité**
- **Disponibilité**

- **Authentification**
- **Traçabilité**
- **Non-répudiation**

Positionnement de la problématique

Qui est concerné par le management de la sécurité d'un système d'information ?

La réponse est simple : tous et chacun des membres de l'organisation à laquelle est rattaché le SI.

- TOUT LE MONDE ! -

L'ensemble du système est aussi sécurisé que son élément le moins sécurisé.

Malgré les meilleures technologies, les équipes informatiques et de sécurité ne peuvent pas protéger les organisations contre elles même. Tous les trous de sécurité qui semblent négligeables isolément peuvent servir à atteindre le système dans sa globalité.

Positionnement dans un système de management de la sécurité

Plusieurs intervenants et équipes ont en charge des aspects différents de la sécurité, par exemple :

- Chaque employé doit se conformer au règlement intérieur de l'entreprise ;
- Les managers doivent s'assurer que les personnes dont ils ont la charge sont informés de leurs devoirs vis-à-vis du système d'information ;
- Les équipes informatiques mettent en place des mécanismes de sécurisation du système d'information ;
- Les services administratifs produisent les documents d'information qui encadrent l'usage du SI ;
- ...

Terminologie de la cryptologie

Terminologie - positionnement des disciplines

- Cryptologie : « science du secret »
- Cryptographie : s'attache à la manipulation de la représentation de l'information pour satisfaire des besoins de sécurité.
- Cryptanalyse : analyse des résultats de processus issus de la cryptographie pour en défaire les services de sécurité.

Différencier

- *Cryptographie* : transforme un message en clair contenant une information secrète en cryptogramme
- *Stéganographie* : cherche à dissimuler l'existence même de l'information secrète

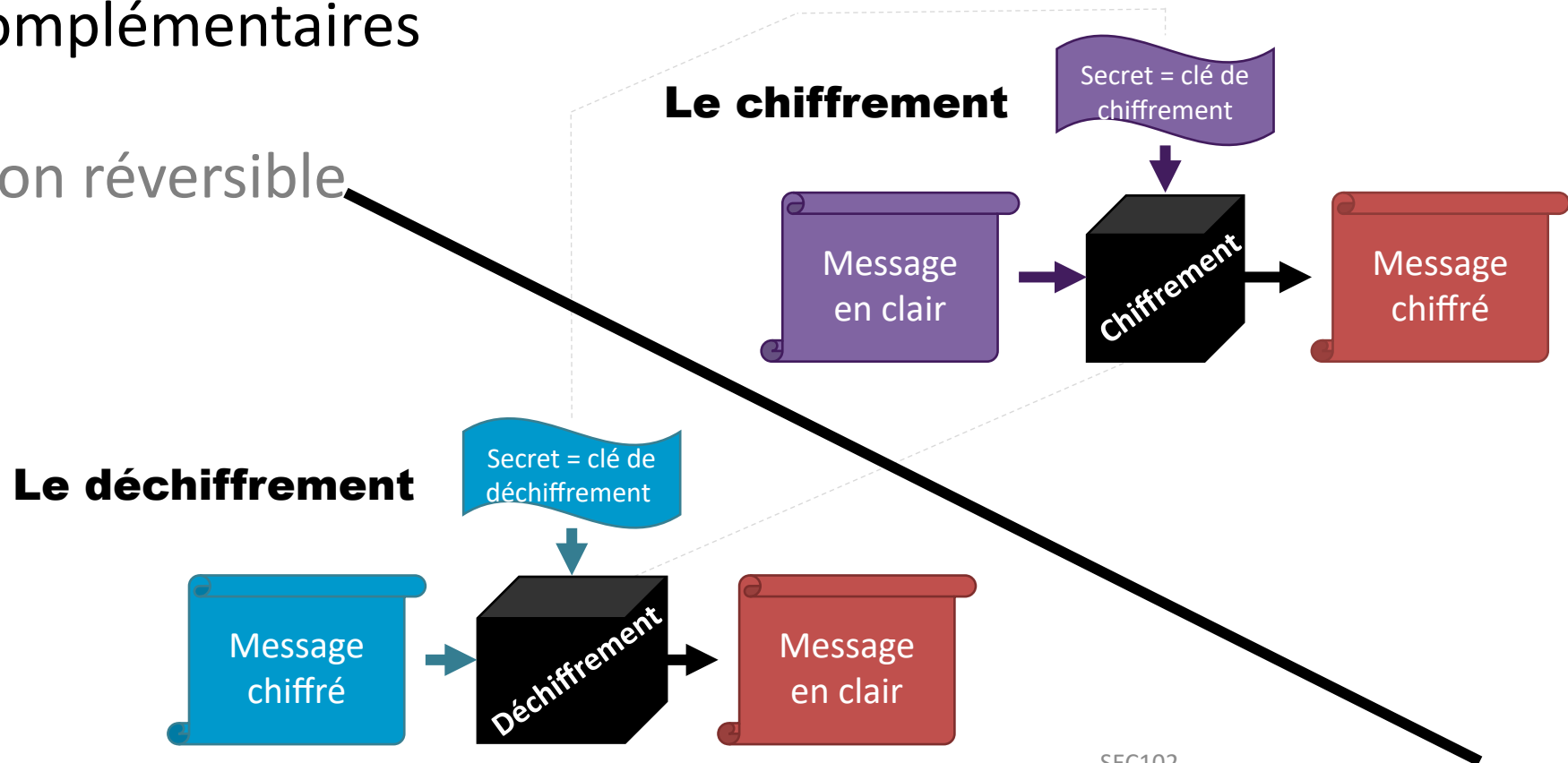
Le chiffrement

Une boîte pour chiffrer / une boîte pour déchiffrer

Le chiffrement

2 procédures complémentaires

Une opération réversible



SEC102

Menaces informatiques et codes malveillants : analyse et lutte

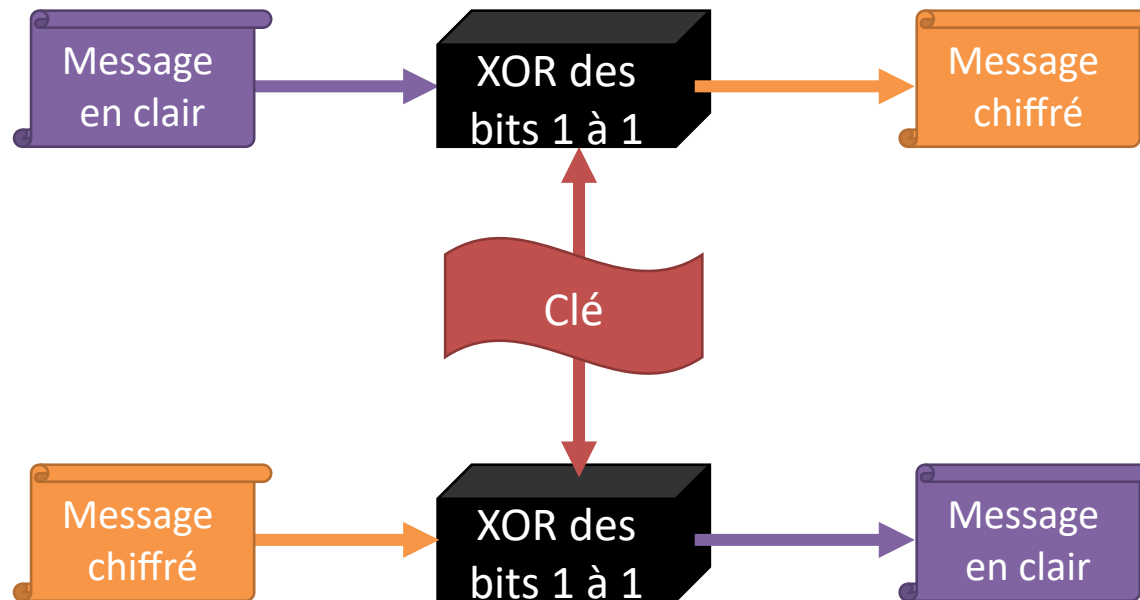
Le chiffrement

De la problématique à la technologie

Le chiffrement parfait

Le chiffrement parfait existe : l'opérateur binaire XOR
... mais son utilisation pour la sécurisation est absurde

Table de vérité de l'opérateur XOR		
<i>a</i>	<i>b</i>	<i>a XOR b</i>
0 (faux)	0 (faux)	0 (faux)
0 (faux)	1 (vrai)	1 (vrai)
1 (vrai)	0 (faux)	1 (vrai)
1 (vrai)	1 (vrai)	0 (faux)



Contraintes à respecter :

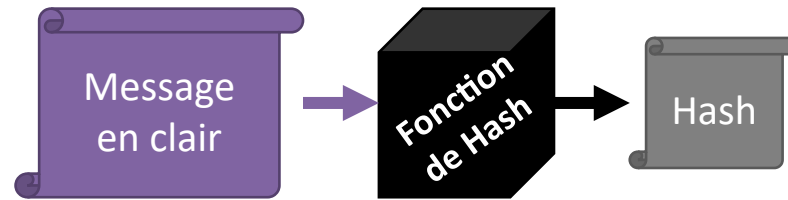
- Chaque bit de la clé a une probabilité parfaitement équivalente entre prendre la valeur 0 et 1
- La clé doit avoir au moins la même taille que le message
- Une clé ne peut être réutilisée pour plusieurs messages

La fonction de hachage

La définition en cryptographie

Le hachage

Une opération non réversible



$$\begin{aligned} \text{Hash} : \{0,1\}^* &\rightarrow \{0,1\}^t \\ x &\rightarrow \text{Hash}(x) \end{aligned}$$

Table de hachage

- Coût du calcul de $\text{Hash}(x)$
- Dimensionnement des collisions sur l'ensemble image

Hachage cryptographique

- Résistance au calcul de pré-image
(Etant donné $y = \text{Hash}(x)$ retrouver x)
- Résistance au calcul de seconde pré-image
(Etant donné x , retrouver $x' \neq x$ avec $\text{Hash}(x) = \text{Hash}(x')$)
- Résistance aux collisions
(Trouver x et x' tels que $\text{Hash}(x) = \text{Hash}(x')$)

Quelle opération pour quel usage ?

Chiffrement VS Hachage

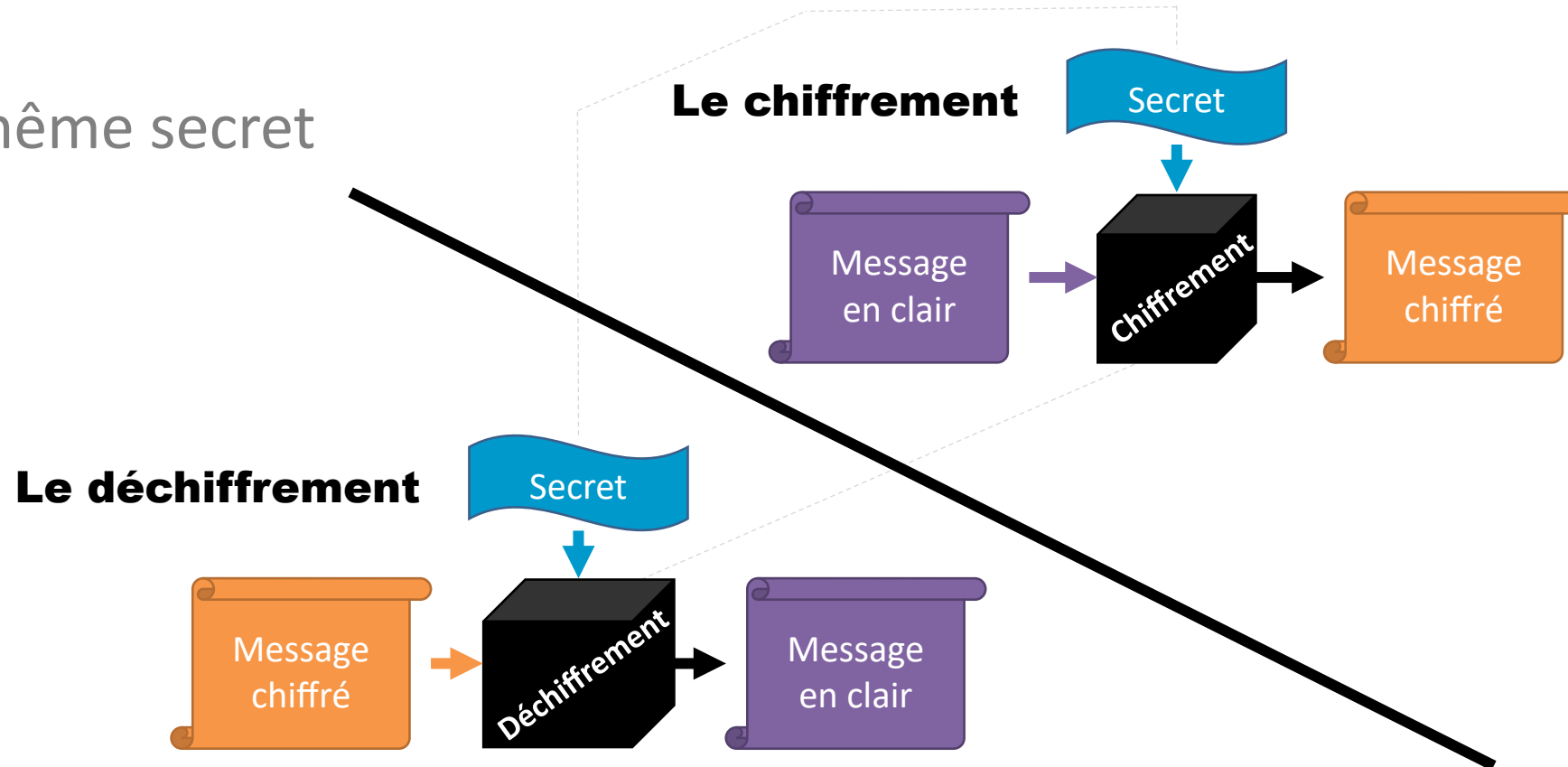
Chiffrement	Hachage
<ul style="list-style-type: none">• Réversible• Lent• Espaces de définition symétriques	<ul style="list-style-type: none">• Non réversible• Rapide• Recouvrement de l'espace des valeurs hachées
<ul style="list-style-type: none">• Lie la possibilité d'accès à l'information à la connaissance du secret	<ul style="list-style-type: none">• Lie la correspondance d'une trace à sa donnée d'origine

2 types de chiffrements ?

SYMÉTRIQUE

Le chiffrement symétrique

Le même secret



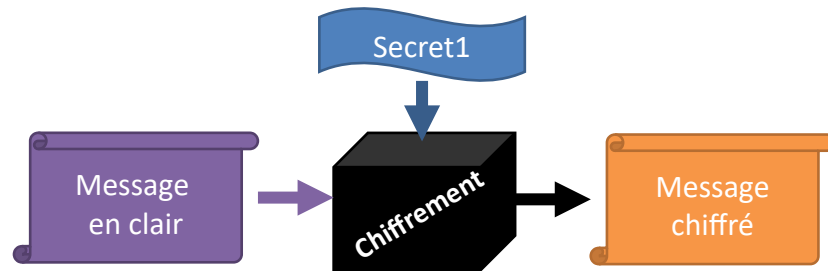
2 types de chiffrement ?

ASYMÉTRIQUE

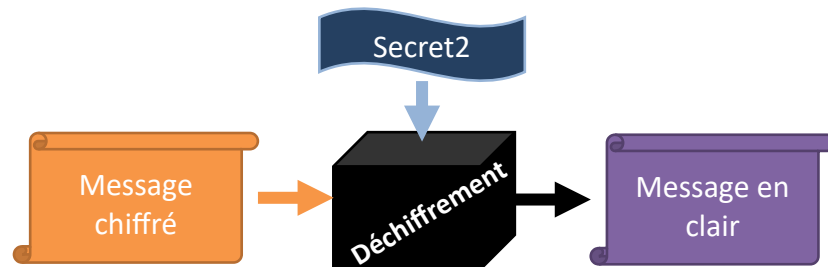
Le chiffrement asymétrique

2 secrets/clés différents

(mais liés)

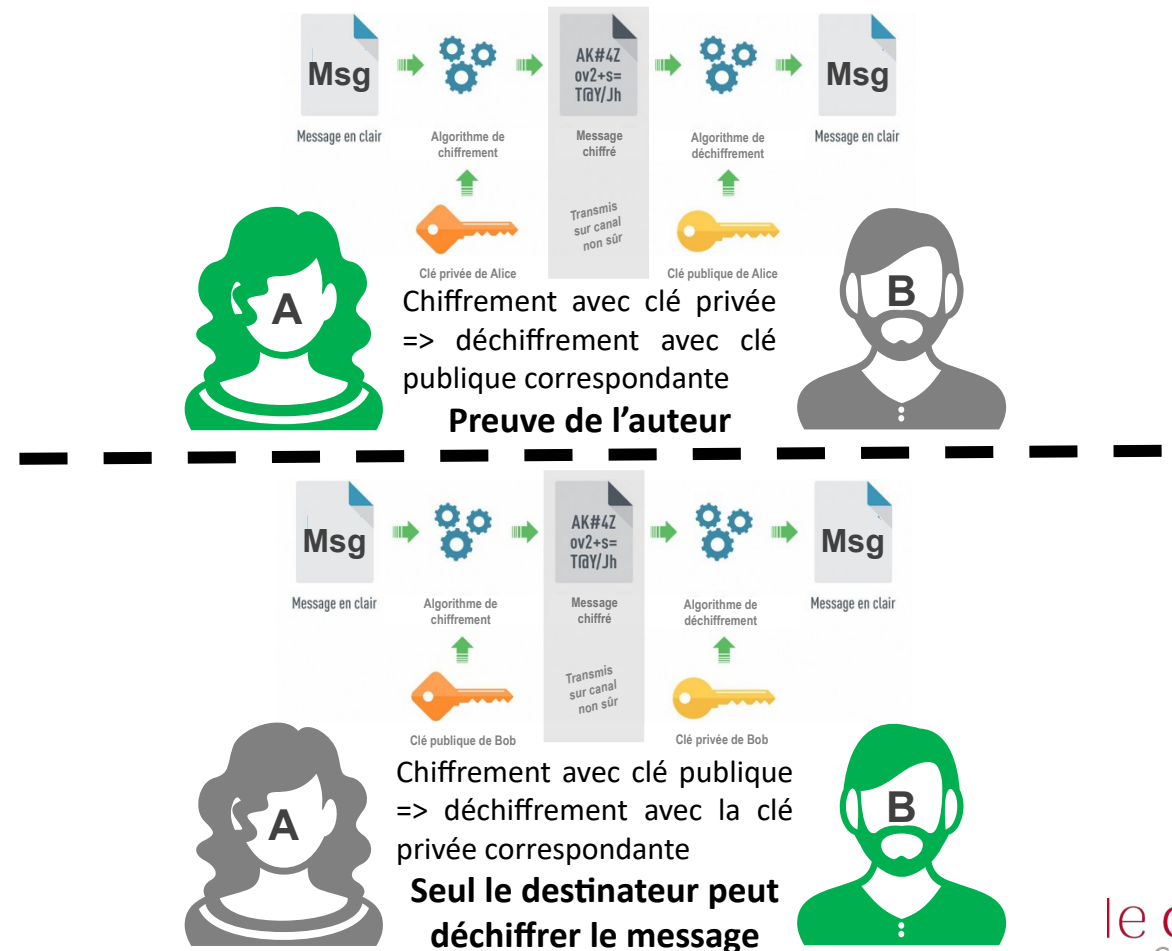


Le chiffrement



Le déchiffrement

Alice envoie un message à Bob



Sécurité informatique

Introduction aux fonctions cryptographiques

Le chiffrement Symétrique VS Asymétrique

Chiffrement Symétrique

- Rapide
- Pour même difficulté de casse de la clé, une petite clé
- Pas de différenciation à l'émission et la réception

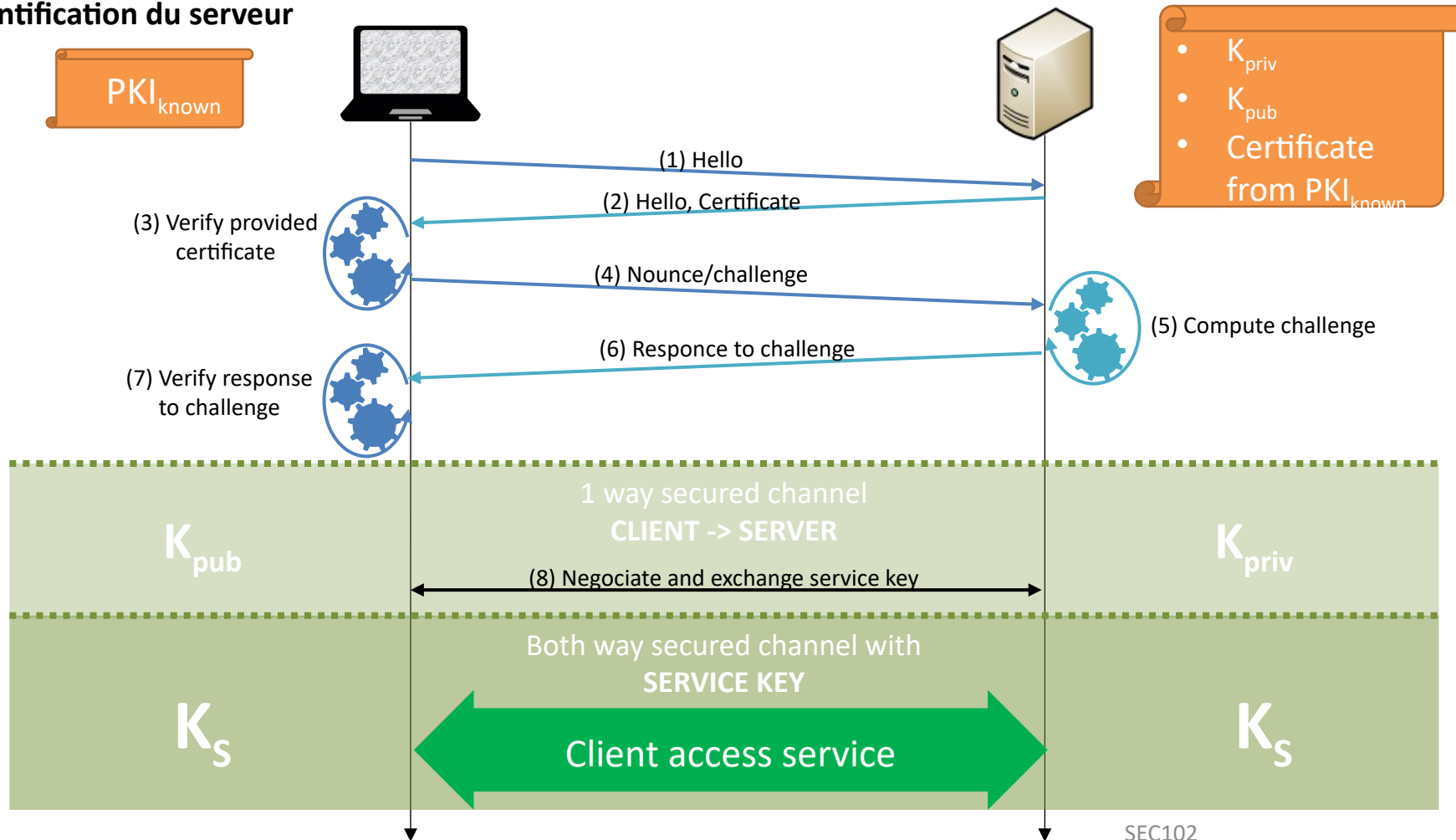
Chiffrement Asymétrique

- Lent
- Pour même difficulté de casse de la clé, une longue clé
- Possibilité de différencier les auteurs ou les destinataires

LES SOLUTIONS TECHNIQUES

Etablissement d'une session SSL/TLS

Un système d'authentification du serveur
- SSL/TLS



SEC102

Menaces informatiques et codes malveillants : analyse et lutte

1. Typologies des codes et des effets

1. Typologies des codes et des effets

VIRUS

Un virus est un morceau de programme informatique malicieux, conçu et écrit pour qu'il se reproduise. Cette capacité à se répliquer, peut toucher votre ordinateur, sans votre permission et sans que vous le sachiez. En termes plus techniques, le virus classique s'attachera à un de vos programmes exécutables et se copiera systématiquement sur tout autre exécutable que vous lancez.

VERS

Un ver (ou worm) est un type de virus particulier. Concrètement, il s'agit de programmes capables de se répliquer à travers les terminaux connectés à un réseau, puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.

De nos jours, c'est essentiellement la messagerie qui sert de vecteur de propagation.

1. Typologies des codes et des effets

LES CHEVAUX DE TROIE

Un cheval de Troie (ou trojan) est un programme qui, introduit dans une séquence d'instructions normales, prend l'apparence d'un programme valide. Mais il contient en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire. A la différence d'un ver, le cheval de Troie ne se réplique pas : il peut demeurer inoffensif, à l'intérieur d'un jeu ou d'un utilitaire, jusqu'à la date programmée de son entrée en action.

KEYLOGGERS

Un keylogger est un logiciel qui enregistre les frappes au clavier pour voler, par exemple, un mot de passe.

1. Typologies des codes et des effets

ROOTKITS

Un rootkit est un « *kit* » pour devenir "*root*"(administrateur) d'une machine. C'est un code malicieux vraiment complexe qui se greffe sur une machine, et parfois le noyau même du système d'exploitation. Il est ainsi capable de prendre le contrôle total d'un PC sans laisser de trace. Sa détection est difficile, parfois même impossible tant que le système fonctionne. Autrement dit, c'est une série de programmes qui permettent au pirate de s'installer sur une machine (déjà infecté ou exploitant une faille de sécurité) et d'empêcher sa détection. Une fois en place, le rootkit est véritablement le maître du système.

HOAX

On appelle **hoax** (en français *canular*) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Ainsi, de plus en plus de personnes font suivre (anglicisé en *forwardent*) des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple :

- provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes

1. Typologies des codes et des effets

RANSOMWARE

Le malware de rançonnage, ou ransomware, est un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et exige le paiement d'une rançon en échange du rétablissement de l'accès. Les premières versions de ransomwares ont été développées à la fin des années 1980. À cette époque, la rançon devait être envoyée par courrier postal. Aujourd'hui, les auteurs de ransomwares demandent à être payés en cryptomonnaies ou par carte de crédit.

CRYPTOJACKING

Le cryptojacking, ou minage de cryptomonnaie est un type de malware qui détourne les ressources matérielles du hôte cible pour contribuer au minage de cryptomonnaie.

Apparu quasiment en même temps que les crypto monnaie, on le retrouve souvent dans des scripts utilisées sur des pages web infectées.

1. Typologies des codes et des effets

ADWARE

Un publiciel (adware) est un logiciel gratuit dont le créateur finance ses activités en affichant de la publicité lors de l'utilisation du logiciel

PHISHING

L'hameçonnage (phishing), est une application d'ingénierie sociale effectuée par courrier électronique pour faire au destinataire une action qui lui est nuisible comme révéler un mot de passe ou transférer une somme d'argent à un fraudeur.

1. Typologies des codes et des effets

SPYWARE

Un espioniciel (en anglais spyware) est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois mouchard) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (on parle de profilage).

Les récoltes d'informations peuvent ainsi être :

- la traçabilité des URL des sites visités,
- Le « traquage » des mots-clés saisis dans les moteurs de recherche,
- l'analyse des achats réalisés via internet,
- voire les informations de paiement bancaire (numéro de carte bleue / VISA)
- ou bien des informations personnelles.

FIN SEQUENCE 1

2. Etudes des modes d'action des codes malveillants

2.1 - Analyse intrinsèque des codes malveillants

2.2 - Anatomies d'attaque type

2.3 - Exemples

2.1- Analyse intrinsèque des codes malveillants

Les logiciels qui « remplissent délibérément les intentions nuisibles d'un attaquant » sont qualifiés de logiciels malveillants.

- <https://www.sans.org/posters/tips-for-reverse-engineering-malicious-code/>
- <https://www.sans.org/posters/malware-analysis-and-reverse-engineering-cheat-sheet/>

L'ISO 27037 - Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques

L'ISO 27042 - Lignes directrices pour l'analyse et l'interprétation de preuves numériques

- <https://cobaz-afnor-org.proxybib-pp.cnam.fr/>

En tant qu'étudiants, vous avez la possibilité d'aller sur les sites physiques de l'AFNOR et de consulter les normes

- Montpellier : <https://www.afnor.org/occitanie/>
- Marseille : <https://www.afnor.org/provence-alpes-cote-d-azur-et-corse/>

2.1- Analyse intrinsèque des codes malveillants

Analyse statique

- L'analyse d'un programme malveillant **sans l'exécuter** se nomme l'analyse statique.
- Les modèles de détection utilisés en analyse statique sont la comparaison de **signatures de chaîne de caractères**, séquence **d'octets n-grams** (pour *operational code*), appels syntaxiques de **bibliothèque**, diagramme de **flux de contrôle**, **fréquence de distribution** des opcodes.
- L'exécutable malveillant doit être déchiffré ou décompressé pour procéder à une analyse statique

Analyse dynamique

- Analyser le **comportement** d'un code malveillant (les interactions avec le système) pendant qu'il est exécuté dans un environnement contrôlé (machine virtuelle, simulateur, émulateur, sandbox, etc) est appelé analyse dynamique
- Cette analyse dévoile le comportement naturel du malware.

2.1- Analyse intrinsèque des codes malveillants

Analyse statique

- Nécessite de connaître le format du fichier (Ex : Format PE, EXIF,...)
- Faible risque de contamination (le code n'est pas exécuté)
- Certaines informations ne seront pas accessibles

Analyse dynamique

- Nécessite l'analyse en environnement protégé (VM, Sandbox, ...)
- Fort risque de contamination (le code est exécuté)
- Certaines informations deviennent accessibles

TP N°2 : UserAssist

Modalité :

- Préparation : 30 min
- Présentation : 10 min

<https://www.aldeid.com/wiki/Windows-userassist-keys>

<https://www.scitepress.org/papers/2017/64167/64167.pdf>

Que contient la clé de registre

`HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\ ?`

Expliquer le principe de ROT13

Réaliser un programme permettant d'implémenter ROT13 (codage et décodage)

- L'utilisateur choisi le mode : codage (message clair) ou décodage (message en ROT13)
- L'utilisateur indique son message dans le mode choisi
- Vous lui retournerez le message dans le mode inverse

Décoder une des valeurs de UserAssist

FIN SEQUENCE 2

TP N°3 : ROT13

Modalité :

- Préparation : 30 min
- Présentation : 10 min

En vous aidant du TP N°2, améliorez votre programme pour que celui-ci permette :

- De récupérer les valeurs de `HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\` dans un fichier qui sera nommé `userassist.txt`
- La lecture du fichier `userassist.txt` Le decode du fichier `userassist.txt` avec le retour en clair dans un fichier qui sera nommé `decode_userassist`.

TP N°4 :

Comparaison des types d'analyse

Modalité :

- Préparation : 30 min
- Présentation : 10 min

Ce TP va vous permettre de constituer votre boîte à outils même si pour le moment vous ne savez peut-être pas comment les utiliser. Il vous appartiendra de la faire vivre tout au long de son cycle de vie.

A partir du lien donné, vous déterminez:

- les avantages et les inconvénients de l'analyse statique et de l'analyse dynamique
- Les logiciels gratuits pouvant être utilisés pour réaliser les analyses
- [https://fr.wikipedia.org/wiki/Analyse de s logiciels malveillants](https://fr.wikipedia.org/wiki/Analyse_de_s_logiciels_malveillants)

FIN SEQUENCE 3

2.1- Analyse intrinsèque des codes malveillants

Obfuscation

- L'obfuscation, assombrissement, ou obscurcissement est une stratégie de gestion de l'information qui vise à obscurcir le sens qui peut être tiré d'un message. Cette stratégie peut être intentionnelle ou involontaire.
- L'obfuscation n'utilise pas d'algorithme de chiffrement.
- Il ne faut pas :
 - Qu'une donnée apparaisse dans le binaire
 - Qu'une donnée apparaisse en mémoire lors de l'exécution
 - Une donnée apparaisse en registre lors de l'exécution
- http://serge.liyun.free.fr/serge/sources/cours_obfuscation.pdf
- https://www.sstic.org/media/SSTIC2014/SSTIC-actes/obfuscation_de_code_python_amlioration_des_techne/SSTIC_2014-Article-obfuscation_de_code_python_amlioration_des_techneiques_existantes-eyrolles_guelton.pdf
- http://igm.univ-mlv.fr/~dr/XPOSE2013/introduction_analyse_malware/obfuscation.html#introduction

2.1- Analyse intrinsèque des codes malveillants

Obfuscation

Il ne faut pas :

- Qu'une donnée apparaisse dans le binaire
- Qu'une donnée apparaisse en mémoire lors de l'exécution
- Une donnée apparaisse en registre lors de l'exécution

L'obfuscation impacte :

- Le temps d'exécution
- La taille du binaire
- La consommation mémoire
- La structure du programme

Propriétés :

- **Conservatif** : Le code doit avoir le même comportement
- **Furtivité** : Rendre l'obfuscation difficile à déceler

Exemples :

- XOR
- Base64

2.1- Analyse intrinsèque des codes malveillants

Magic Number

- En informatique, le terme ***magic number*** peut désigner :
 - une constante numérique ou un ensemble de caractères utilisé pour désigner un format de fichier ou un protocole ;
 - une constante numérique non nommée ou mal documentée ;
 - un ensemble de valeurs ayant un sens particulier (par exemple, les GUID).

[https://fr.wikipedia.org/wiki/Nombre_magique_\(programmation\)](https://fr.wikipedia.org/wiki/Nombre_magique_(programmation))

https://en.wikipedia.org/wiki/List_of_file_signatures

<https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5>

<https://www.media.mit.edu/pia/Research/deepview/exif.html>

<https://docs.microsoft.com/fr-fr/windows/win32/wic/-wic-native-image-format-meta-data-queries>

TP N°5 : Etude du Format PE

Modalité :

- Préparation : 30 min
- Présentation : 10 min

https://fr.wikipedia.org/wiki/Portable_Executable

- Rédigez un résumé explicatif et visuel du format PE
- Quelles sont les extensions de fichiers qui ont un format PE ?
- Quelle signature HEXA le format PE prend-il ?
- Sous quels SE retrouve-t-on le format PE ?
- Que se passe t-il si Windows ne reconnaît pas le format PE pour le fichier ?
- Dans quelle partie de la structure PE, trouve-t-on le **TimeStamp** ?
 - A quoi cela correspond-il ?
 - Est-ce utile pour une analyse de fichier ?
- Combien peut-il y avoir de Section dans le format PE ?
- Dans quelle partie de la Section trouve-t-on le code du programme ?
- Qu'est-ce qu'un packer et à quoi peut-il servir ?
- Quels logiciels peuvent vous aider à analyser un fichier au format PE ?

FIN SEQUENCE 4

Ressources complémentaires

- Windows Forensics Analysis
- Devenir analyste de malwares

TP N°6 : Comprendre l'outil d'analyse

Modalité :

- Préparation : 30 min
- Présentation : 10 min

Ce TP va vous permettre de vous confronter à l'apprentissage d'un nouvel outil sans forcément pouvoir bénéficier d'une formation spécifique. Cela vous permettra de constituer votre 1^{ère} procédure d'utilisation, qu'il faudra faire vivre durant son cycle de vie.

- Téléchargez
 - CFF Explorer <https://ntcore.com/files/ExplorerSuite.exe>
 - PE Studio <https://www.winitor.com/download>
- Vous en ferez la présentation des deux logiciels (avantages, inconvénients, portables, multiplateformes, ...)
- Vous chercherez, adapterez ou réaliserez un tutoriel / procédure d'utilisation (simple) permettant à vos collaborateurs d'utiliser seul un de ces logiciels

FIN SEQUENCE 5

TP N°7 : Analyse statique

Modalité :

- Préparation : 30 min
- Présentation : 10 min

http://igm.univ-mlv.fr/~dr/XPOSE2013/introduction_analyse_malware/analyse_statique.html

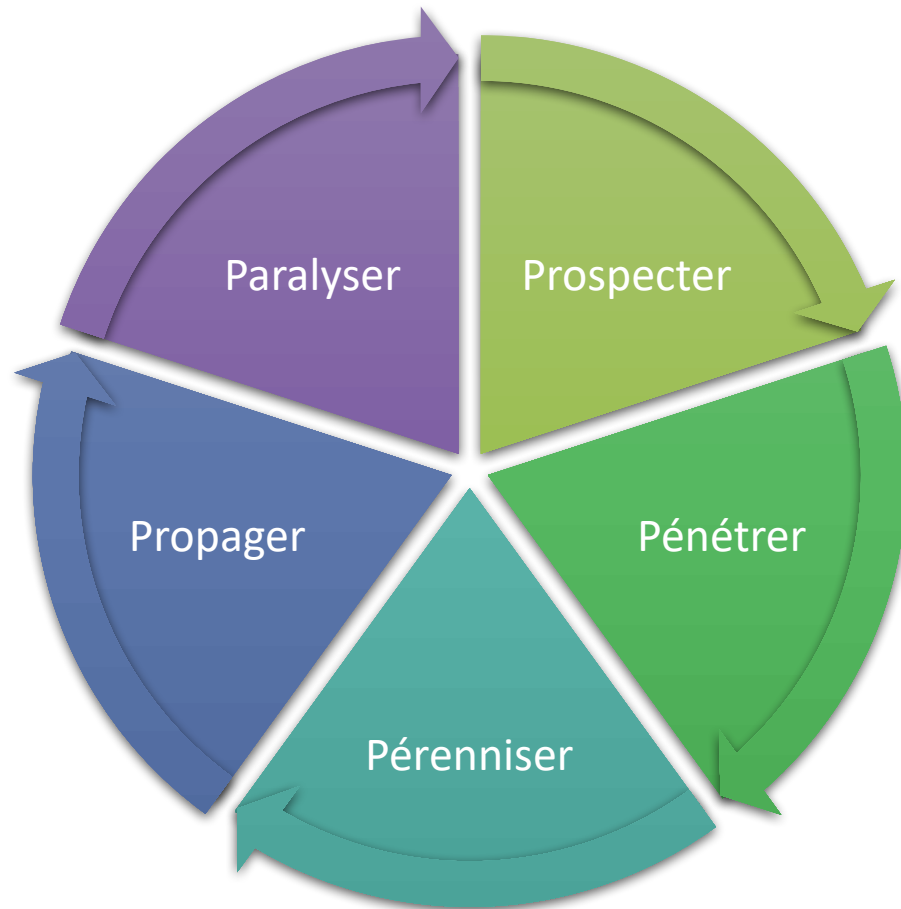
- Quelle norme ISO convient-il d'utiliser pour réaliser une analyse statique ou dynamique ? Et pourquoi est-ce nécessaire ?
 - Aidez-vous du chapitre 7 de la norme ISO 27042
- Télécharger la suite d'outils Sysinternals avec le lien donné <https://download.sysinternals.com/files/SysinternalsSuite.zip>
- A partir des outils collectés dans le TP précédent et du tuto, vous ferez l'analyse statique de **procexp.exe** contenu dans la Suite Sysinternals :
 - Nom du fichier, taille, date de compilation, propriétaire,...
 - Signature (hash), quelle est son utilité ?
 - Examinez Les chaînes de caractères (Unicode, ASCII), trouvez-vous des informations intéressantes et pour le sont-elles ?
 - Les interactions que l'outil peut avoir avec le SE (ex: création de clé registre,...) ?
- Vous analyserez le fichier (AffichezMoi) mis à disposition par la secrétaire. Le fichier ne s'ouvre pas.

2.2- Anatomie d'une attaque type

Pour qu'une attaque soit menée à bien, une attaque passe par plusieurs phases :

- **Prospecter / Probe** : Dans un premier temps, une personne mal intentionnée va chercher les failles pour pénétrer le réseau. Nous parlons alors de collecte d'informations. Le but de cette étape est d'établir une cartographie du réseau et d'obtenir le maximum de détails (Nom de domaine, NetBIOS, IP, Services, ...). La collecte se fait autant sur le SI que sur l'Humain, qui est fortement vulnérable à l'Ingénierie Sociale (Social Engineering)
- **Pénétrer / Penetrate** : Une fois une ou plusieurs failles identifiées, le pirate va chercher à les exploiter afin de pénétrer au sein du SI. Si le pirate obtient qu'un accès à un utilisateur sans privilège, il tentera d'obtenir l'accès à un compte possédant des droits administratifs.
- **Péreniser / Persist** : Le réseau infiltré, le pirate cherchera à y revenir facilement. Pour cela, il installera par exemple des back doors, cherchera à récupérer la base login/mdp afin de se reconnecter ultérieurement ou encore en se créant un compte avec privilèges. Cependant, en général, il corrigera la faille par laquelle il s'est introduit afin de s'assurer qu'aucun autre pirate n'exploitera sa cible.
- **Propager / Propagate** : Le réseau est infiltré et l'accès est persistant. Le pirate pourra alors explorer le réseau et trouver de nouvelles cibles qui l'intéresseraient. Au cas où le pirate serait parvenu jusqu'à ce point, la seule bonne nouvelle est qu'il est possible de détecter la suite des attaques avec Snort.
- **Paralyser / Paralyze** : Les cibles identifiées, le pirate va agir et nuire au sein du SI.

2.2- Anatomie d'une attaque type



- **Prospector** : Se renseigner à partir de sources disponibles (documents, pas web,...), organigramme, cartographie, informations sur le personnel (facebook, ...), scan de ports, fingerprinting, bannières,...
- **Pénétrer** : utiliser les vulnérabilités détectées (Application, Web, SQL, Injection de Code,...)
- **Pérenniser** : Backdoor, code malveillant,...
- **Propager** : malware,...
- **Paralyser** : récupération des données, modification des données, utilisation des ressources, ...

FIN SEQUENCE 6

TP n°8 : Wannacry

Modalité :

- Préparation : 30 min
- Présentation : 10 min

- A partir du lien donné, vous complétez le tableau ci-dessous
 - <https://attack.mitre.org/software/S0366/>

	N° Technique	Explications
Prospecter		
Pénétrer		
Pérenniser		
Propager		
Paralyser		

3. Lutte contre le code malveillant

3.1 - Veille

3.2 - Alerte

3.3 - Détection des effets des codes

3.4 - Identification de la menace

3.1- VEILLE : Protéger ses biens essentiels

- En cybersécurité, la phase de veille est l'une des plus importante. Une mauvaise analyse du contexte peut amener à mettre les ressources humaines et matérielles au mauvais endroit.
- Elle permet :
 - D'identifier son écosystème
 - Repérer et suivre ses fragilités
 - Identifier et caractériser les menaces
- Elle porte sur :
 - Le Système d'Information
 - La réputation
 - L'environnement économique, politique et Social

3.1- VEILLE : Protéger ses biens essentiels

- Présentation de NISSUS Home (Version Gratuite)
 - <https://fr.tenable.com/downloads/nessus>
- NISSUS est un scanner de vulnérabilité. Il vous permettra :
 - d'identifier votre Ecosystème
 - Repérer et suivre ses fragilités
 - Identifier et caractériser les menaces
- Il fonctionne grâce à un moteur de base de vulnérabilités qu'il conviendra de mettre à jour régulièrement

3.1- VEILLE : Protéger ses biens essentiels

Nessus - Récupération

Commencer par créer un dossier (ex : nessus), dans lequel vous y déposerez les fichiers téléchargés.

1. Enregistrez-vous via le formulaire à droite de la page
2. Cliquez sur **Download** pour accéder à la page de téléchargement
3. Téléchargez la version de **Nessus pour Windows** ainsi que le **checksum** associé et nommez le **checksum.txt**

3.1- VEILLE : Protéger ses biens essentiels

Nessus - Vérification

Après avoir récupéré le fichier d'installation il faut vérifier son intégrité. Pour cela nous allons calculé le checksum de l'exécutable à celui fourni par l'éditeur.

1. Placez-vous dans le dossier contenant les fichiers téléchargés précédemment.
2. Maintenez la touche **Maj** et faites un **clic droit** de souris, sous les fichiers
3. Sélectionnez **Ouvrir la fenêtre Powershell ici...**
4. Tapez la commande **Get-Filehash .\Nessus-x.y.z-x64.msi >> resultat.txt**
 - **Nessus-x.y.z-x64.msi** : version de Nessus que vous venez de récupérer
 - **>> resultat.txt** : indique que vous redirigez le résultat vers un fichier nommé resultat.txt (qui se trouvera dans le dossier de récupération des fichiers)

3.1- VEILLE : Protéger ses biens essentiels

Nessus - Vérification

Laissez la fenêtre PowerShell ouverte et allez dans le dossier de récupération des fichiers. Vous devriez y voir un nouveau fichier, resultat.txt

1. Ouvrir le fichier **checksum.txt** et copiez le résultat du Hash SHA256
2. Retournez sur la fenêtre PowerShell et ouvrez les guillemets puis collez le résultat copié précédemment. Fermez les guillemets.
3. Ouvrez maintenant le fichier **resultat.txt** et copiez le résultat du hash et retournez à votre fenêtre PowerShell.
4. Ajoutez un espace après la fermeture des guillemets, ajouter **-eq**, ouvrez les guillemets , collez le résultat copié précédemment. Fermez les guillemets.
5. Vous devez avoir une commande de ce type : **"hash_fichier checksum.txt" -eq "hash_fichier resultat.txt"**
6. Validez. Si vous obtenez **TRUE**, cela signifie que vous avez récupéré le fichier de l'éditeur.

3.1- VEILLE : Protéger ses biens essentiels

Nessus - installation

Vous devez avoir reçu un email, vous indiquant votre clé d'activation. Copiez cette clé, elle sera nécessaire.

1. Placez-vous dans votre dossier de récupération.
2. Double cliquez sur **Nessus-x.y.z-x64.msi**
3. **Nessus** : Next - I accept the terms in the licence agreement – Next – Next – Next – Install
4. **WinPcap** : Next – I Agree - Automatically start the WinPcap driver at boot time – Install – Finish
5. Finish

3.1- VEILLE : Protéger ses biens essentiels

Nessus - initialisation

Suite à l'installation, votre navigateur doit s'ouvrir sur <http://localhost:8834/WelcomeToNessus-Install/welcome>

1. Cliquez sur **Connect via SSL - Ajouter une exception... - Confirmer l'exception de sécurité**
2. Indiquez un **login** et **mot de passe** – Continue – **Home, Professional or Manager** – Collez votre **clé de licence** – Continue
3. Patientez...

3.1- VEILLE : Protéger ses biens essentiels

Nessus - utilisation

L'initialisation est terminée, vous allez pouvoir passer à la découverte de l'EcoSystème de votre SI.

Cette découverte permet de :

- Etablir un état des lieux,
- Cibler les vulnérabilités et
- D'appliquer les mesures correctives

Un attaquant procède de la même façon mais son but n'est pas d'appliquer les mesures correctives mais d'utiliser les vulnérabilités / failles, pour compromettre votre SI

3.1- VEILLE : Protéger ses biens essentiels

Nessus - utilisation

Découverte de l'EcoSysteme

(<https://www.it-connect.fr/adresses-ipv4-et-le-calcul-des-masques-de-sous-reseaux/>)

1. Créez un nouveau dossier nommé **EcoSysteme** en cliquant sur **New Folder**
2. Se placer dans le dossier **EcoSysteme** et cliquez sur **New Scan** et sélectionnez **Host Discovery**
3. **Onglet Settings – BASIC - General**
 - Name : Libellé du scan
 - Folder : EcoSysteme
 - Target : 192.168.1.0/24
4. **Onglet Settings – DISCOVERY**
 - Scan Type : Port scan (all ports)
5. **Onglet Settings – REPORT**
 - Cochez tout sauf **Display unreachable hosts**
6. **Save**, revenez dans le dossier **EcoSysteme** et lancez le scan que vous venez de créer.

3.1- VEILLE : Protéger ses biens essentiels

Nessus - utilisation

Recherche des Vulnérabilités

1. Placez-vous dans le dossier **EcoSysteme** et cliquez sur **New Scan** et sélectionnez **Basic Network Scan**
2. **Onglet Settings – BASIC - General**
 - Name : Libellé du scan
 - Folder : EcoSysteme
 - Target : 192.168.1.0/24
3. **Onglet Settings – DISCOVERY**
 - Scan Type : Port scan (all ports)
4. **Onglet Settings – ASSESSMENT**
 - Scan Type : **Scan for all web vulnerabilities (complex)**
5. **Onglet Settings – REPORT**
 - Cochez tout sauf **Display unreachable hosts**
6. **Onglet Settings – ADVANCED**
 - Scan Type : Scan low bandwidth links
7. **Save**, revenez dans le dossier **EcoSysteme** et lancez le scan que vous venez de créer.

TP N°9 : Veille

Modalité :

- Durée variable

- A l'aide des explications données en cours et de Nessus (ou autre logiciel), vous ferez :
 - L'inventaire de votre écosystème
 - La recherche des vulnérabilités et les correctifs (est-ce toujours possible ?)
 - Identifiez et caractérisez les menaces
 - Pensez-vous que votre inventaire est exact ? Justifiez
 - Pensez-vous que le fait de disposer d'un parc avec des matériels identiques est un avantage ou un inconvénient ? Justifiez en donnant des exemples.

FIN SEQUENCE 7

3.2- ALERTE : Défendre les actifs

- En cybersécurité c'est dans cette phase que l'entraînement est nécessaire.
- Elle permet :
 - Surveiller les sources de menaces
 - Détecter des attaques dans les événements
 - Alerter en fonction de l'impact
- Pour cela, il faut comprendre d'où viennent les menaces afin de mettre en place les moyens d'alertes efficaces.
- Pour cela on peut mettre en place :
 - Un SOC (Security Operations Center), qui sera chargé de détecter et prévenir les incidents de sécurité, tout en tenant compte des besoins de disponibilité du SI

3.2- ALERTE : Défendre les actifs

CERT et CSIRT

<https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/>

L'appellation CSIRT est privilégiée en Europe, CERT étant une marque déposée aux États-Unis par l'université Carnegie-Mellon.

CERT : Computer Emergency Response Team

CSIRT : Computer Security Incident Reponse Team

C'est quoi ? :

- un centre d'alerte et de réaction aux attaques informatiques

Mission :

- centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations;
- traitement des alertes et réaction aux attaques;
- établissement et maintenance d'une base de données des vulnérabilités ;
- prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- coordination éventuelle avec les autres entités (hors du domaine d'action)

Comment ? :

- En mettant à disposition les informations des bulletins de sécurité

3.2- ALERTE : Défendre les actifs

CERT et CSIRT

En France

- <https://www.cert.ssi.gouv.fr/>
- <https://www.cert.ssi.gouv.fr/csirt/intercert-fr/>

Autres Pays

- https://fr.wikipedia.org/wiki/Computer_emergency_response_team

3.2- ALERTE : Défendre les actifs

0-Day

https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day

<https://fr.wikipedia.org/wiki/Vupen>

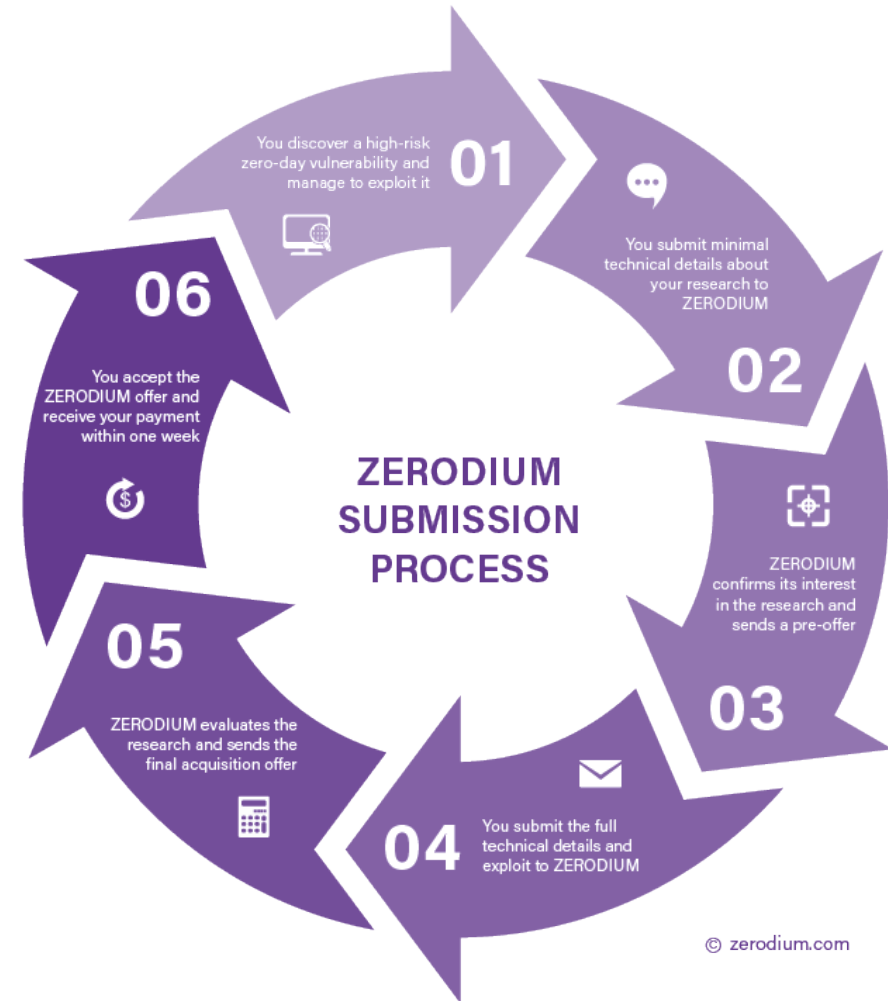
<https://zerodium.com/program.html>

- Dans le domaine de la sécurité informatique, une **vulnérabilité *zero-day*** — également orthographiée **0-day** — (en français : « jour zéro ») est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive.
- La terminologie « *zero day* » ne qualifie pas la gravité de la faille : comme toute vulnérabilité, sa gravité dépend de l'importance des dégâts pouvant être occasionnés, et de l'existence d'un exploit, c'est-à-dire d'une technique « exploitant » cette faille afin de conduire des actions indésirables sur le produit concerné.

3.2- ALERTE : Défendre les actifs

0-Day

<https://zerodium.com/program.html>

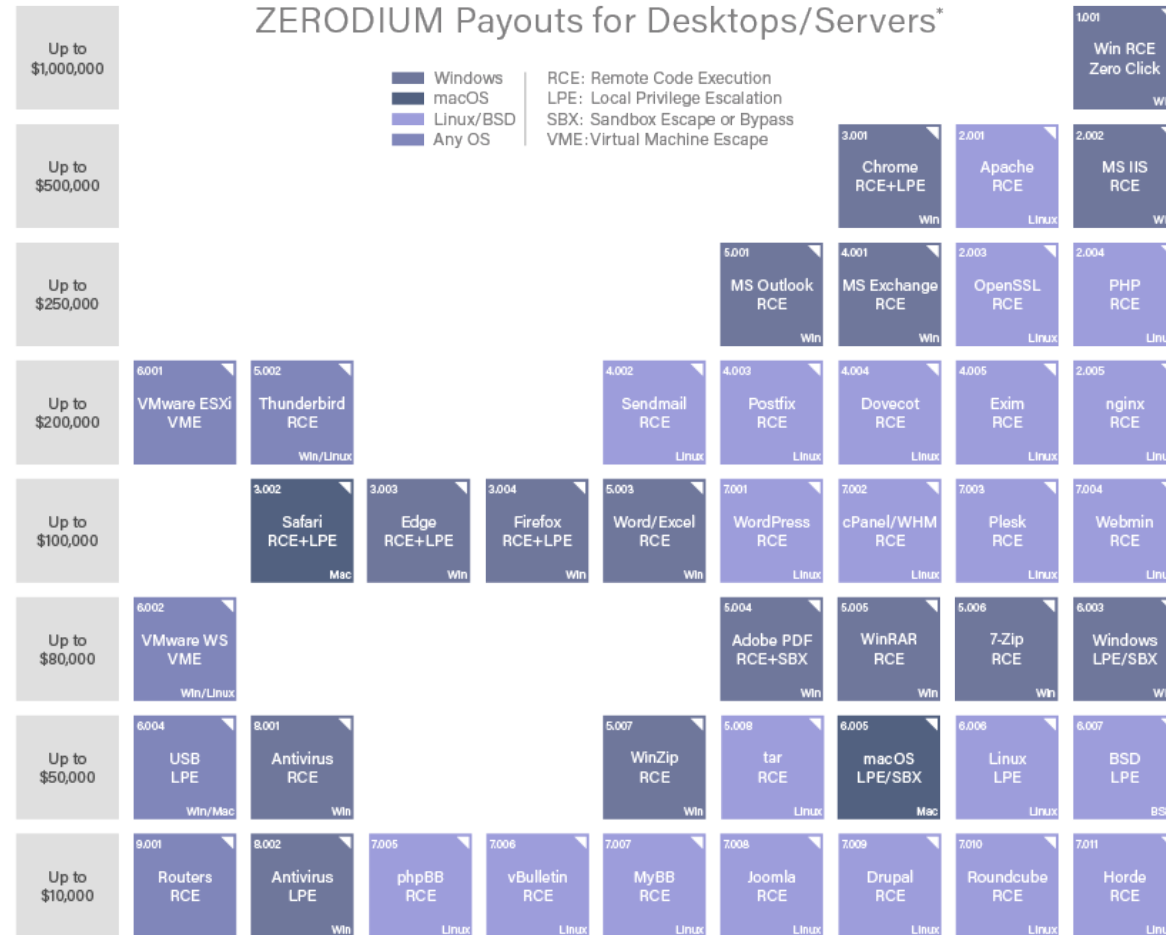


SEC102

Menaces informatiques et codes malveillants : analyse et lutte

3.2- ALERTE : Défendre les actifs

0-Day



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

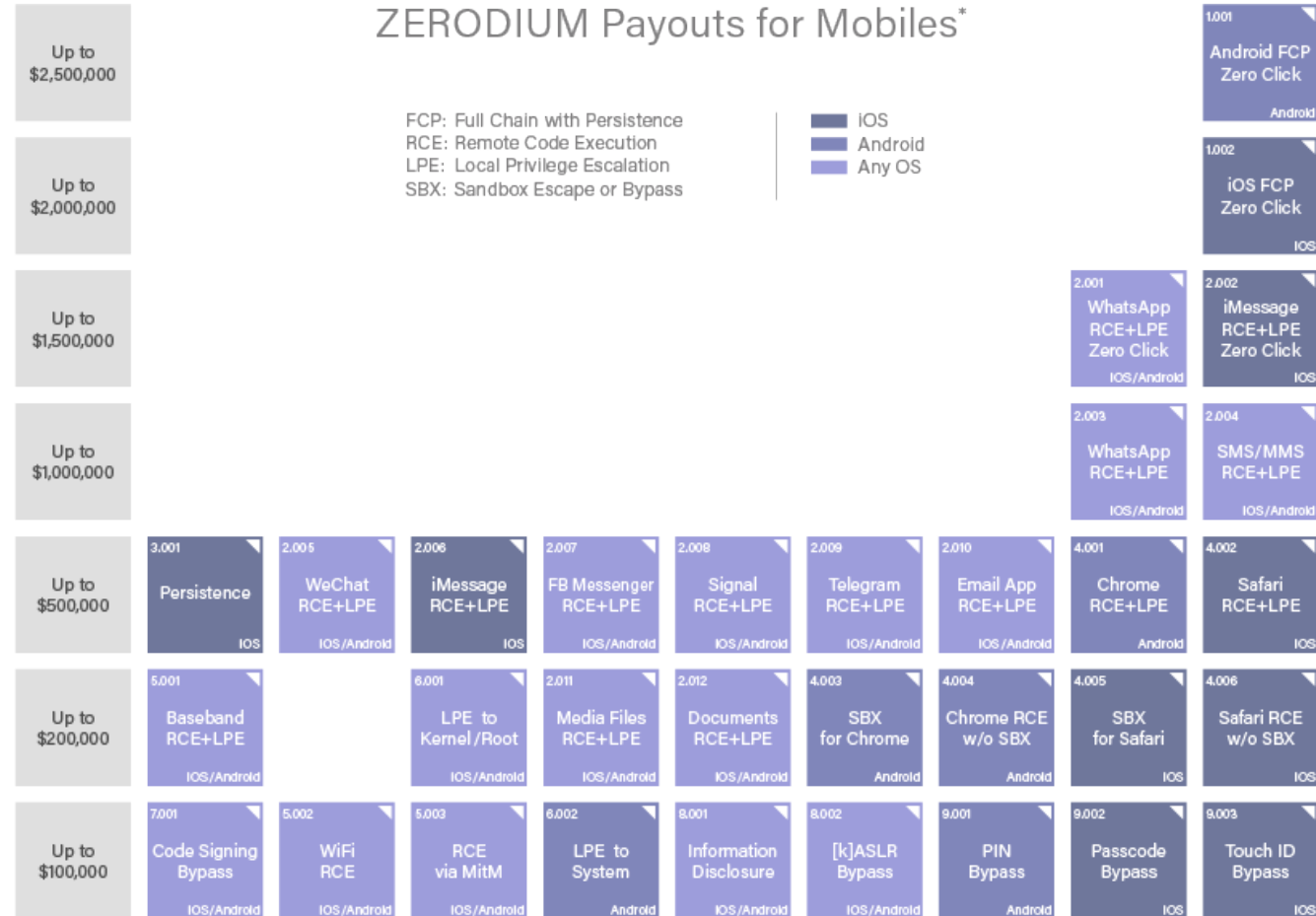
2019/01 © zerodium.com

SEC102

Menaces informatiques et codes malveillants : analyse et lutte

3.2- ALERTE : Défendre les actifs

0-Day



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

SEC102

Menaces informatiques et codes malveillants : analyse et lutte

3.2- ALERTE : Défendre les actifs

- Présentation de SNORT
 - <https://www.snort.org/>
- Snort est un IDS (Intrusion Detection System), il vous permettra :
 - Surveiller les sources de menaces
 - Détecter des attaques dans les événements
 - Alerter en fonction de l'impact
- Snort fonctionne avec des bases de menaces qu'il convient de mettre à jour régulièrement. Il est aussi possible de créer ses propres règles afin d'être au plus proche des besoins du terrain.

3.2- ALERTE : Défendre les actifs

Snort – Présentation

SNORT est un système de détection d'intrusion.

Snort est capable d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocole, recherche/correspondance de contenu et peut être utilisé pour détecter une grande variété d'attaques et de sondes comme des dépassements de buffers, scans, attaques sur des CGI, sondes SMB, essai d'OS fingerprintings et bien plus.

Pour effectuer ces analyses, SNORT, se fonde sur des règles. Snort est fourni avec certaines règles de base mais cependant, comme tout logiciel, SNORT n'est pas infallible et demande donc une mise à jour régulière.

3.2- ALERTE : Défendre les actifs

Snort - Fonctionnement

SNORT fonctionne principalement en ligne de commande mais peut se voir ajouter un module graphique. Il se base sur une série de règles écrites par la communauté ou sur des règles personnalisées.

L'ensemble de la configuration se fait dans le fichier **snort.conf**

Une fois la configuration mise en place, SNORT

- Ecoute le réseau
- Compare les trames aux signatures de règles
- Alerte en cas de détection

3.2- ALERTE : Défendre les actifs

Snort - Récupération

Commencer par créer un dossier (ex : snort), dans lequel vous y déposerez les fichiers téléchargés.

<https://www.snort.org/downloads>

Vous pouvez vous enregistrer via **Sign-In** en haut droite de la page mais cela est facultatif

1. Cliquez sur **Download - Snort** pour accéder à la page de téléchargement
2. Téléchargez la version de **Snort pour Windows** ainsi que le **checksum** associé et nommez le **checksum_snort.txt**
3. Cliquez sur **Download – Rules** pour accéder à la page de téléchargement des règles
4. Téléchargez **community-rules.tar.gz** et le checksum associé et nommez le **checksum_snort_rules.txt**

3.2- ALERTE : Défendre les actifs

Snort - Vérification

De la même façon que vous avez procédé pour Nessus, il faut vérifier les checksums des fichiers.

Attention les checksums sont en MD5, il faudra l'indiquer dans la commande PowerShell.

Voici les commandes

- **Get-Filehash -Algorithm MD5 .\Snort_x.y.z_Installer.exe >> resultat_snort.txt**
- **Get-Filehash -Algorithm MD5 .\ community-rules.tar.gz >> resultat_snort_rules.txt**
- **« hash_checksum_snort » -eq « hash_resultat_snort.txt »**
- **« hash_checksum_snort_rules » -eq « hash_resultat_snort_rules.txt »**

3.2- ALERTE : Défendre les actifs

Snort - Installation

Placez-vous dans le dossier **snort**

1. Double cliquez sur **Snort_x.y.z_Installer.exe**
2. I Agree – Next – Next – Close – OK

3.2- ALERTE : Défendre les actifs

Snort - Configuration

Rules

Placez-vous dans le dossier **snort**

1. Décompressez le fichier **community-rules.tar.gz**
2. Décompressez le fichier **community-rules.tar**
3. Copiez le fichier **community.rules** dans **c:\snort\rules**
snort.conf

4. Placez-vous dans le dossier **c:\snort\ect**
5. Créez une **copie de sauvegarde** du fichier **snort.conf**
6. Editez le fichier **snort.conf**

C'est dans le fichier **snort.conf**, que vous allez configurer les paramètres de l'application.

3.2- ALERTE : Défendre les actifs

Snort – Configuration

N° ligne	Modification
104	var RULE_PATH ../rules devient var RULE_PATH C:\Snort\rules
105	var SO_RULE_PATH ../so_rules devient var SO_RULE_PATH C:\Snort\so_rules Il faudra aussi créer le dossier so_rules dans c:\snort\
106	var PREPROC_RULE_PATH ../preproc_rules devient var PREPROC_RULE_PATH C:\Snort\preproc_rules
113	var WHITE_LIST_PATH ../rules devient var WHITE_LIST_PATH C:\Snort\rules
114	var BLACK_LIST_PATH ../rules devient var BLACK_LIST_PATH C:\Snort\rules
186	# config logdir : devient config logdir : C:\Snort\log
247	/usr/local/lib/snort_dynamicpreprocessor/ devient C:\Snort\lib\snort_dynamicpreprocessor
250	/usr/local/lib/snort_dynamicengine/libsfe_engine.so devient C:\Snort\lib\snort_dynamicengine\sfe_engine.dll
253	/usr/local/lib/snort_dynamicrules devient C:\Snort\lib\snort_dynamicrules (dossier à créer)
298	unicode.map devient C:\Snort\etc\unicode.map
511	\$WHITE_LIST_PATH/white_list.rules devient \$WHITE_LIST_PATH\white.list Il faudra créer un fichier white.list dans c:\snort\rules
512	\$BLACK_LIST_PATH/black_list.rules devient \$BLACK_LIST_PATH\black.list Il faudra créer un fichier black.list dans c:\snort\rules
534	include classification.config devient include C:\Snort\etc\classification.config
535	include reference.config devient include C:\Snort\etc\reference.config
545 à 651	\$RULE_PATH/ devient \$RULE_PATH\
656 à 661	\$PREPROC_RULE_PATH/ devient \$PREPROC_RULE_PATH\ Retirer le # devant les lignes (pour décommenter)
669 à 686	\$SO_RULE_PATH/ devient \$SO_RULE_PATH\
689	include threshold.conf devient include C:\Snort\etc\threshold.conf
546 à 641	Si vous n'êtes en enregistrez, il faudra mettre toutes les lignes en commentaire car les fichier .rules mentionnés ne seront pas disponibles
544	Ajouter include \$RULE_PATH\community.rules

3.2- ALERTE : Défendre les actifs

Snort - Utilisation

Choisir l'interface à écouter (uniquement Windows)

1. Ouvrez une **invite de commande** en tant qu'**administrateur**
2. Placez-vous dans **c:\snort\bin**
3. Tapez **snort.exe -W**
4. Si vous avez plusieurs interfaces, notez le numéro de la ligne correspondante à votre interface.

Test et rapport sur la configuration snort

5. Tapez **snort.exe -i num_interface -c c:\snort\etc\snort.conf -T**
6. Si les tests fonctionnent correctement, vous devriez avoir les 2 lignes suivantes
 - Snort successfully validated the configuration!
 - Snort exiting

3.2- ALERTE : Défendre les actifs

Snort - Utilisation

Règles locales de test

1. Editez le fichier **C:\Snort\rules\local.rules**
2. Ajoutez les lignes suivantes :
 - alert icmp any any -> any any (msg:"Test ICMP alert"; sid:1000001;)
 - alert udp any any -> any any (msg:"Test UDP alert"; sid:1000002;)
 - alert tcp any any -> any any (msg:"Test TCP alert"; sid:1000003;)
3. Retournez dans votre invite de commande et tapez la commande suivante :
 - **snort.exe -i num_interface -c c:\snort\etc\snort.conf -A console**
4. Si tout se passe bien, vous devriez avoir s'afficher des lignes d'alertes
5. Arrêtez snort avec **Ctrl + C**
6. Retournez dans le fichier **C:\Snort\rules\local.rules** et mettez les lignes en commentaire en ajoutant **#** devant chacune des lignes

3.2- ALERTE : Défendre les actifs

Snort - Infographie

BASIC OUTLINE OF A SNORT RULE

```
[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options] )
```

Rule Header

Rule Header alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any

TP N°10 : ALERTE – Snort

Modalité :

- Durée variable

Reprenez le TP n°8. Vous avez détecté des vulnérabilités.

- Choisissez une vulnérabilité
- A l'aide de Snort, vous créez la (les) règle(s) nécessaire(s) à la surveillance du matériel impacté.
 - Vous ferez un schéma réseau pour expliquer où votre sonde est placée et pourquoi vous avez choisi de la positionner ici
 - Vous expliquerez la vulnérabilité à surveiller
 - Vous expliquerez votre règle et en quoi elle répond au besoin de surveillance
 - N'oubliez pas de joindre le fichier de log

FIN SEQUENCE 8

3.3- Détecter les effets des codes

Un code malveillant aura des effets sur votre système.

C'est ce que l'on nomme des **signaux faibles** :

- Message via fenêtrage (popup, ...)
- Création et/ou lancement de processus, de services, drivers, dll,...
- Saturation du processeur, de la mémoire, du disque
- Ouverture de ports

Les tentatives d'accès au réseau et au système sont elles aussi des signaux faibles. En effet, ce n'est pas parce que vos systèmes de sécurités auront réussi à bloquer les tentatives d'accès qu'il faut pour autant les « éliminer » de la liste des signaux faibles.

- Pourquoi l'attaquant a-t-il choisi de passer par ici ?
- Pourquoi l'attaquant a-t-il utilisé cette technique ?
- ...

3.3- Détecter les effets des codes

La sensibilisation des utilisateurs peut aussi être un moyen d'ALERTE.

Sans entrer dans le détail des codes malveillants, il est intéressant d'expliquer succinctement et/ou graphiquement les effets des codes malveillants.

Un utilisateur sensibilisé sera plus facilement réceptif aux signaux faibles.

La constitution d'un groupe de Relais Informatique peut aussi être un avantage

- Employé volontaire formé au 1^{er} diagnostic (Le câble réseau est-il connecté ? ...)
- Ils sont vos yeux et vos mains en cas d'intervention à distance
- Rassurent les collègues
- Dispose d'un langage « d'informaticien » de base

3.4- Identification de la menace

- L'identification d'un code malveillant est importante.
- Pour identifier une menace il faut mettre en évidence les Indices de Compromission (IOC)
- Les IOC intègrent généralement les signatures des codes malveillants, les adresses IP, les hash MD5 de fichiers malveillants ou d'URL ou encore les noms de domaine des serveurs de commande et de contrôle de botnet.
- Les IOC se trouvent a niveau de la mémoire, des registres, des fichiers,...
- Une fois que les IOC ont été identifiés dans un processus de réponse aux incidents et de criminalistique informatique, ils peuvent être utilisés pour la détection précoce des tentatives d'attaque futures en utilisant des systèmes de détection d'intrusion et un logiciel antivirus.
- Pour un traitement automatisé plus efficace, il existe des initiatives et des outils visant à normaliser le format des IOC afin de permettre leurs échanges entre différentes structures.

3.4- Identification de la menace

Liens utiles

- <https://www.lemagit.fr/tribune/Identifier-des-Indicateurs-Cles-de-Compromission>
- <https://mitre.github.io/unfetter/about/>
- <https://attack.mitre.org/>
- https://stix.mitre.org/language/version1.0/xsddocs/extensions/test_mechanism/open_ioc_2010/1.0/open_ioc_2010_xsd.html
- <https://www.sans.org/posters/memory-forensics-cheat-sheet/>
- <https://www.volatilityfoundation.org/>
- <https://www.sleuthkit.org/>

TP N°11 : Identification de la menace- IOC

Modalité :

- Préparation : 30 min
- Présentation : 10 min

- A partir des liens donnés dans le cours et d'internet, répertoriez les IOC concernant Wannacry
- Quels types d'éléments sont nécessaires pour avoir des IOC efficaces ?
- Compléter votre boîte à outils afin de pouvoir
 - Réaliser une image mémoire (dump mémoire)
 - Réaliser une image disk
 - Analyser un dump mémoire
 - Analyser une image disk
- N'oubliez pas de tester vos nouveaux logiciels

FIN SEQUENCE 9

4. Caractérisation

4.1 - Des impacts techniques

4.2 - Des impacts économiques

4.3 - Des impacts fonctionnels

4.1 – Caractérisation des impacts techniques

Lister les impacts techniques et caractériser les.

4.2 – Caractérisation des impacts économiques

Lister les impacts économiques et caractériser les.

4.3 – Caractérisation des impacts fonctionnels

Lister les impacts fonctionnels et caractériser les.