INFORMATION
TECHNOLOGY
& SOLUTIONS

Cybersécurité
Compléments & Exercices

Roland Inan
Didier Law-Tho

DAUPHINE
UNIVERSITÉ PARIS
PSL

Plan du cours

INFORMATION TECHNOLOGY & SOLUTIONS

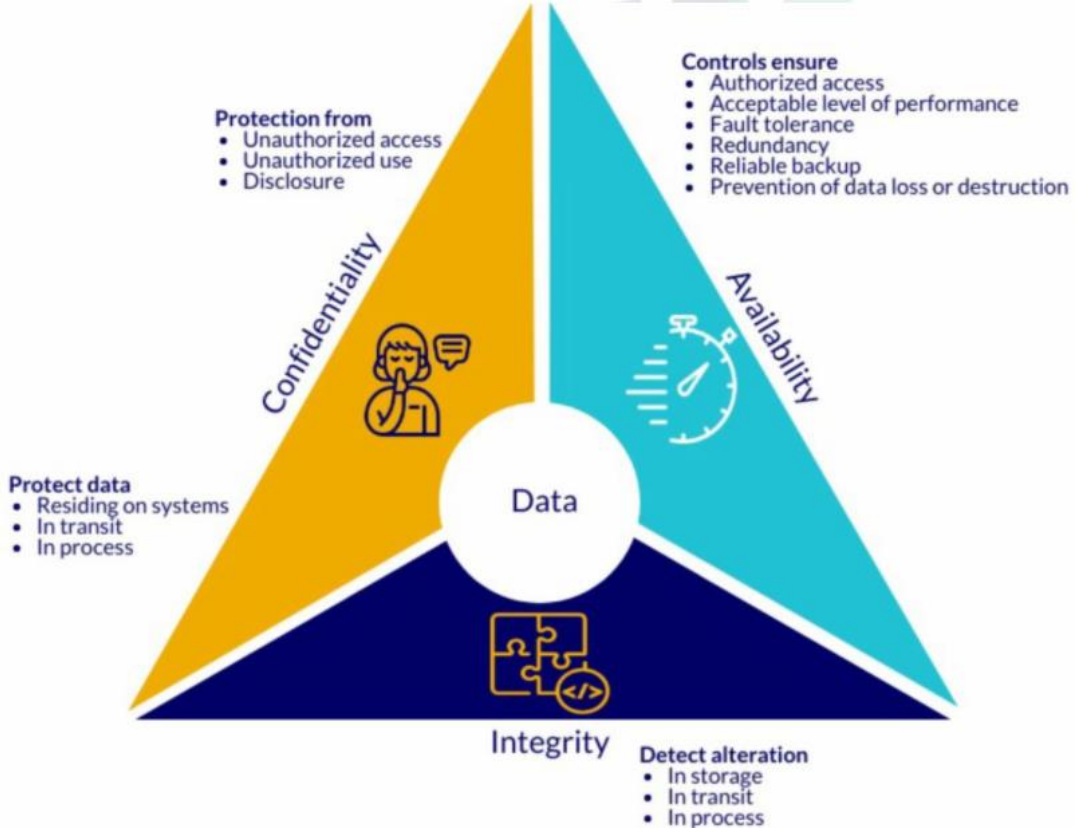
- **Rappels des concepts réseau**
- **Bases de la cryptographie**
- **Composants de sécurité réseau**
  - Zones démilitarisées (DMZ)
  - Serveurs mandataires (Proxies)
  - Pare-feux (Firewalls)
  - VPN (Virtual Private Network)
- **Etude de cas:**
  - Projet de mise en place de services de diffusion vidéo live
- **Perspectives**
  - Introduction à la Cybersécurité

Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. **Notions de base**
2. **Cibles d'attaques sur Internet**
3. **Tactiques de phishing**
4. **Infections par malwares**
5. **Vols de mots de passe et contrôle d'accès**
6. **Attaques réseau**
7. **Attaques du Cloud**
8. **Piratage du réseau sans fil**
9. **Casser le chiffrement**
10. **Analyse de risques**

Le Triptyque CIA



Ce que la cybersécurité n’est pas!

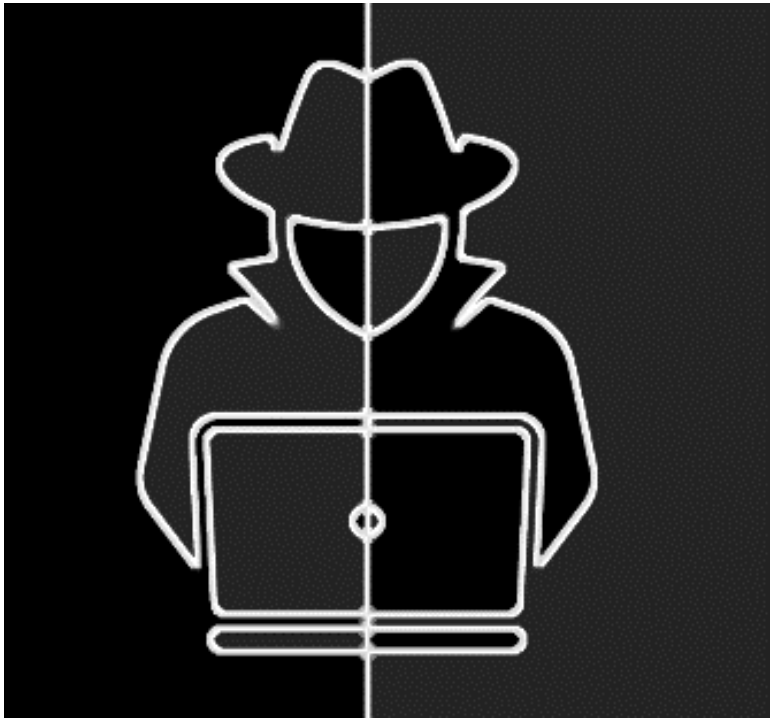
INFORMATION TECHNOLOGY & SOLUTIONS

- **La cybersécurité n’est pas synonyme de piratage**
- **La cybersécurité n’est pas seulement la gestion des équipements réseau ou la sécurisation des systèmes informatiques**
- **La cybersécurité demande plus que des compétences techniques. La communication interpersonnelle est essentielle!**

Black Hats

INFORMATION TECHNOLOGY & SOLUTIONS

- **Script Kiddies**
- **Organisations criminelles**
- **Hacktivistes**
- **Acteurs gouvernementaux**
- **APT (Advanced Persistent Threat)**



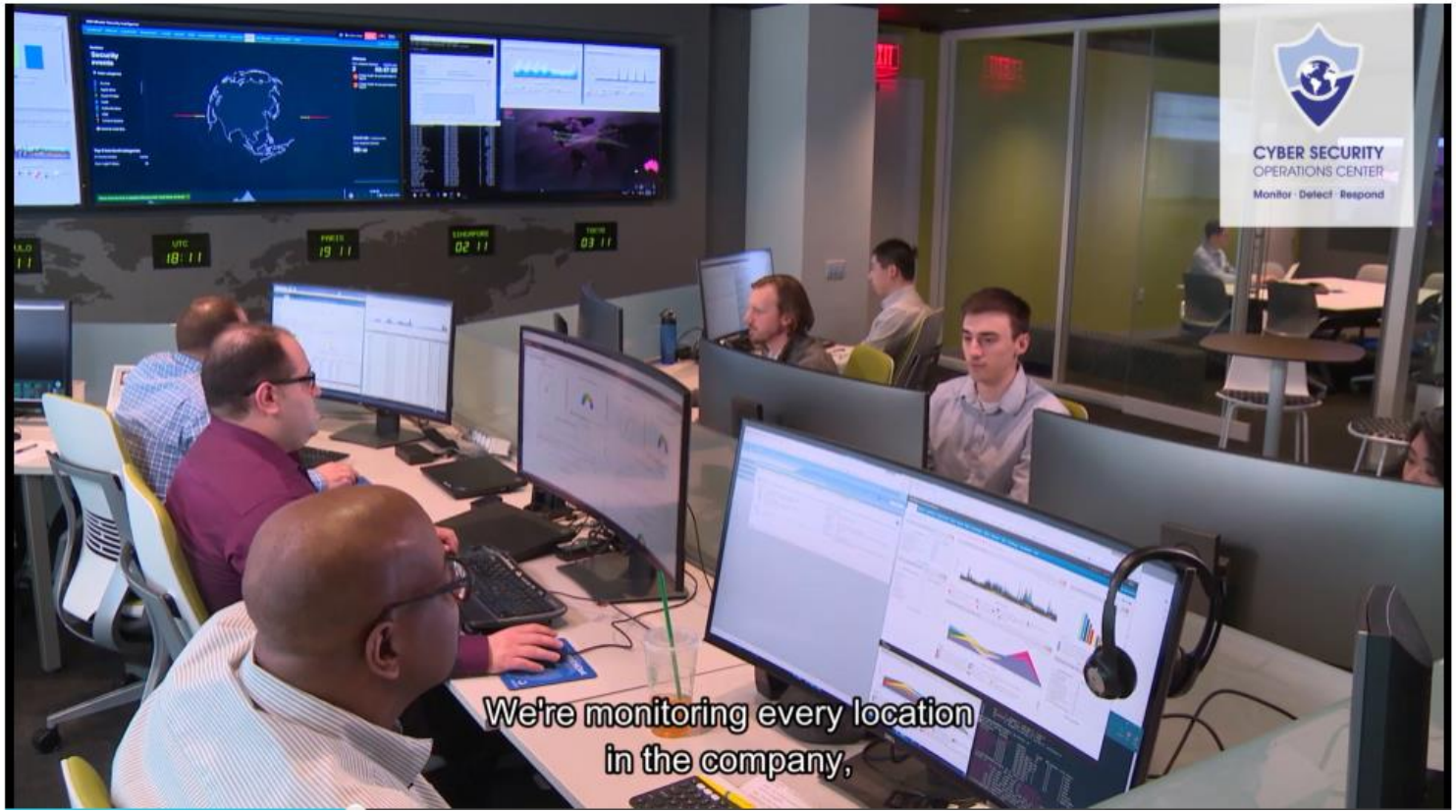
White Hats

INFORMATION TECHNOLOGY & SOLUTIONS

- **Analystes Cybersécurité/Security Operations Center (SOC)**
- **Consultants Cybersécurité**
- **Architectes Cybersécurité**
- **CISO (Chief Information Security Officers) ou RSSI**
- **Gestionnaires d’incidents/vulnérabilités**
- **Chasseurs de menaces**
- **Analystes Forensique**
- **Pentesters**

Sanofi Cyber Security Operations Center

INFORMATION TECHNOLOGY & SOLUTIONS



Exercice*: Rejoignez la Communauté!

INFORMATION TECHNOLOGY & SOLUTIONS

- **Aller plus loin avec la cybersécurité et les menaces**

- **Ressources gouvernementales**
  - ANSSI:https://www.ssi.gouv.fr/
  - NIST: https://csrc.nist.gov/
  - CISA: https://www.cisa.gov/
  - NICE: https://www.nist.gov/itl/applied-cybersecurity/nice

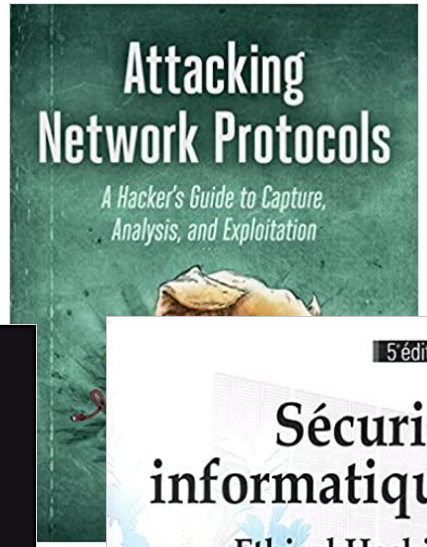
- **Information sur les menaces**
  - MITRE ATT&CK®: https://attack.mitre.org/
  - MS-ISAC: https://www.cisecurity.org/ms-isac/
  - InfraGard: https://www.infragard.org/
  - SANS Internet Storm Center: https://isc.sans.edu/

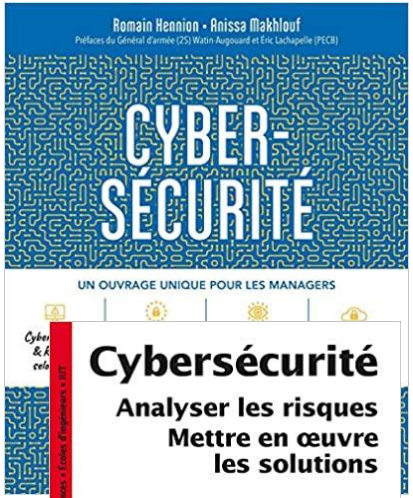
- **Blogs Cybersécurité:**
  - Krebs on Security: https://krebsonsecurity.com/
  - Threatpost: https://threatpost.com/
  - FireEye blog : https://www.fireeye.com/blog.html

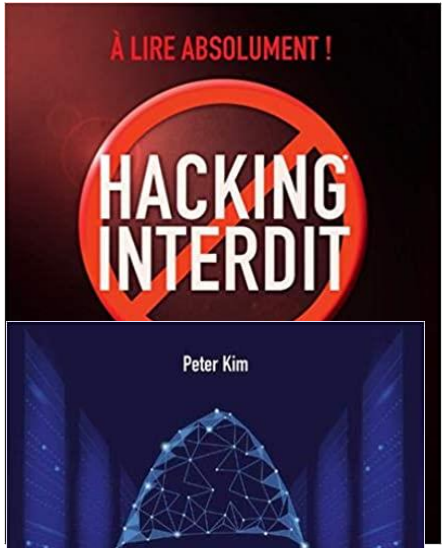
- **Podcast Cybersécurité**
  - Security Now: https://twit.tv/shows/security-now
  - Darknet Diaries: https://darknetdiaries.com/

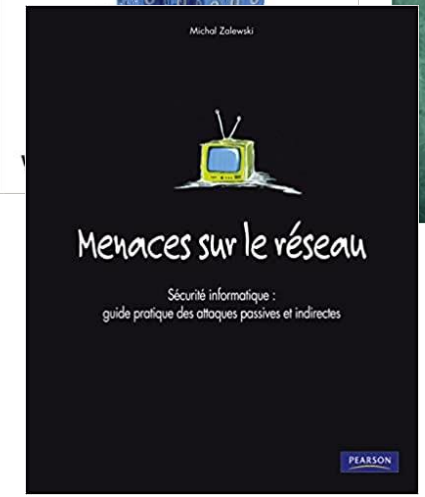
Et aussi quelques bonnes feuilles!

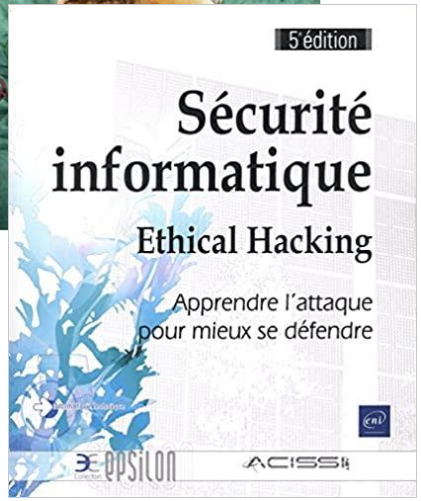
INFORMATION TECHNOLOGY & SOLUTIONS

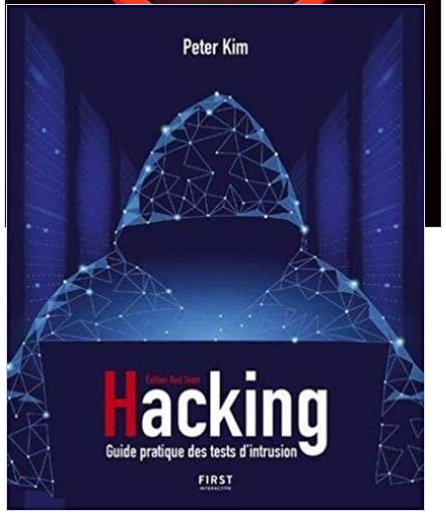












Cybersécurité - Compléments et Exercices

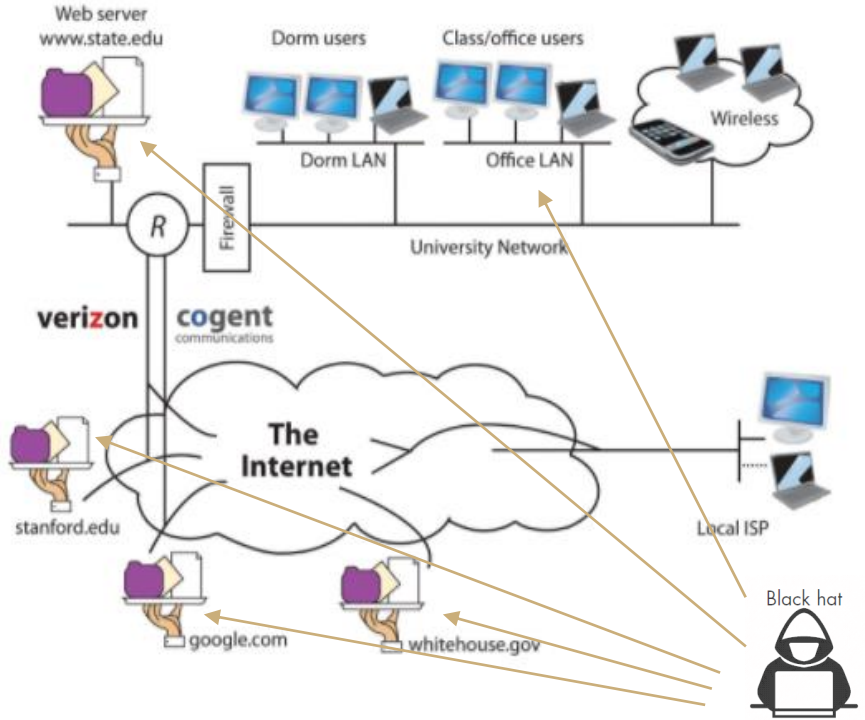
INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Comment fonctionne Internet?

INFORMATION TECHNOLOGY & SOLUTIONS

- **TCP/IP est la colonne vertébrale d'internet**
- **Réseaux Privés versus Publics**
- **Internet du point de vue du pirate**
  - Comment passer depuis le côté public vers le côté privé?

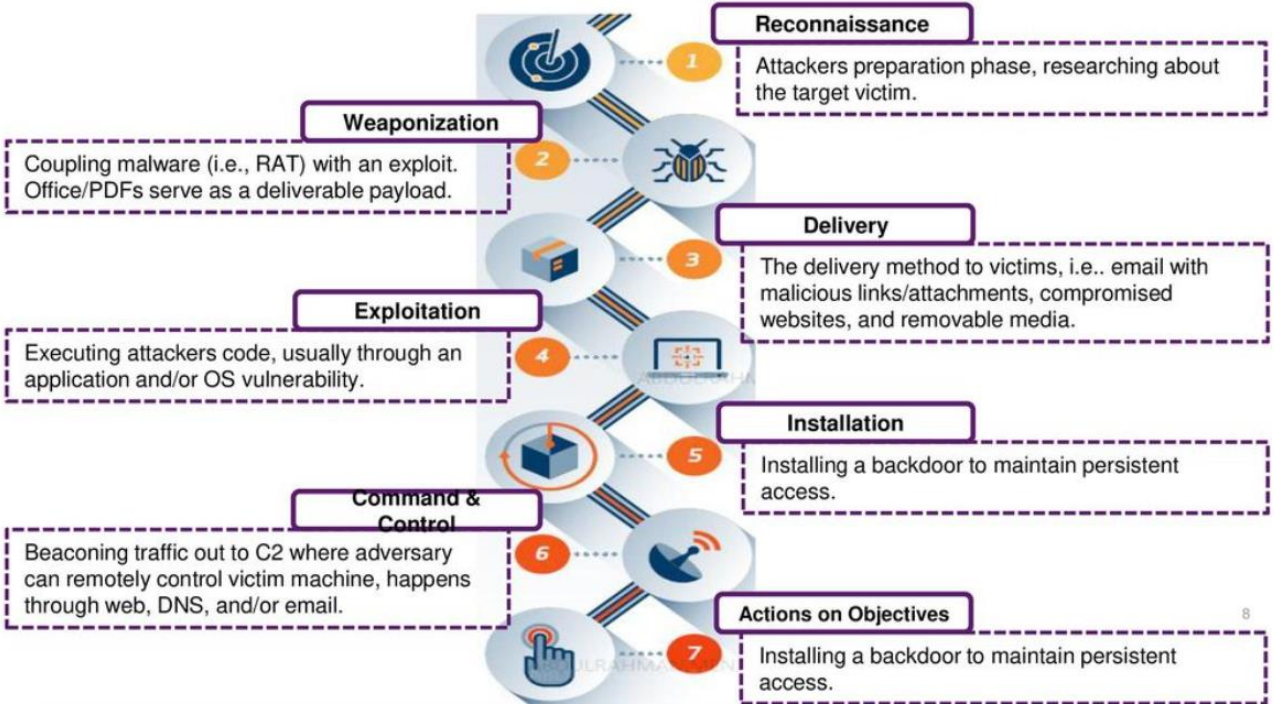


Méthodologie d'attaque

INFORMATION TECHNOLOGY & SOLUTIONS

- **Exemple du Lockheed Martin Cyber Kill Chain (CKC)**

A Term Derived from Offensive Military Tactics, Coined by Lockheed Martin (LM)
Allows for Proactive Remediation & Mitigation of Advanced Threats
A 7-Step Approach Depicting Stages of any Cyber Attack:



Comment un pirate choisit sa cible?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Exemple d'acquisition ou de fusion d'une entreprise**
  - Actualités et informations sur la vie des entreprises
  - Scans des sites webs pour trouver des adresses mail
  - Récupération des offres d'emploi comme un administrateur système avec des connaissances sur un type spécifique de serveur Web.
  - Exploitation des informations d'enregistrements publics (range d'@IPs attribuées à l'entreprise)
  - Mise au point d'une attaque effective en utilisant une faille connue et obtenir l'accès au serveur.

- **Exemple de traque sur les réseaux sociaux**
  - Objectif pénétrer le réseau d'une entreprise très sécurisée
  - Attaque latérale sur une société partenaire de la cible
  - Fouille sur Linkedin et Facebook pour identifier un employé du département informatique de l'entreprise partenaire
  - Traque sur Twitter (geolocalisation) et social engineering pour récolte d'informations sensibles (incident sécurité sur un serveur de messagerie)
  - Attaque sur l'entreprise partenaire via la faille identifiée et accès sur le réseau de la cible via la relation de confiance – Installation d'un backdoor

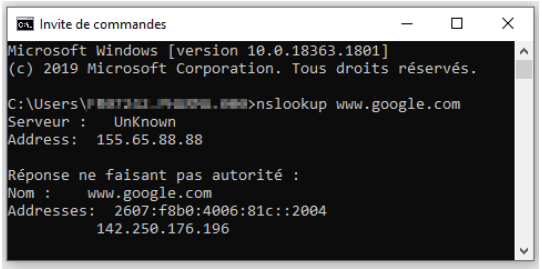
Comment se cacher des pirates?

INFORMATION TECHNOLOGY & SOLUTIONS

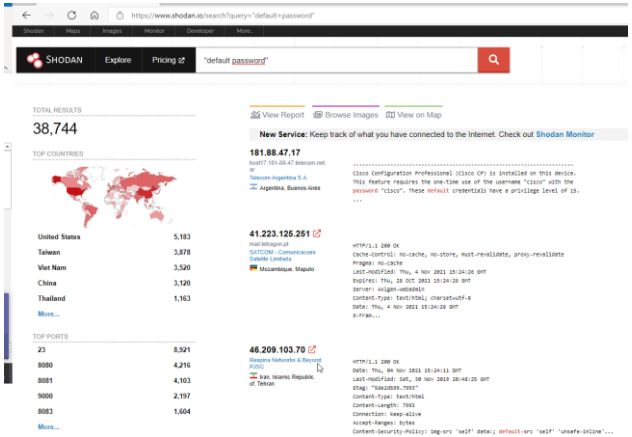
- **Implémenter la sécurité opérationnelle (OPSEC)**
  - Processus de compréhension et de minimisation des informations qui peuvent être utilisées contre vous
- **Garder toujours en tête les 3 règles suivantes quand vous postez une information sur internet:**
  - L'internet est **ouvert**
    - Requêtes DNS sur des protocoles non chiffrés
  - L'internet est **public**
    - https://who.is/
  - L'internet est **éternel**
    - https://archive.org/

Exercice*: Analyser votre réseau

- **Outils réseau de commande en ligne (Win10/MacOS)**
  - ipconfig / ifconfig
  - nslookup www.google.com / nslookup www.google.com
  - ping 8.8.8.8 / ping –c 4 8.8.8.8
  - Tracert 8.8.8.8 / traceroute 8.8.8.8



- **Utiliser SHODAN**
  - https://www.shodan.io/
  - Mot de passe par défaut
    - Telnet



Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Qu’est-ce que le Phishing?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Le phishing ou hameçonnage est une des attaques de social engineering les plus communes**
- **C’est une tentative pour manipuler sa victime pour lui faire révéler des informations critiques, habituellement par la messagerie**
- **Le pirate essaie de se faire passer pour une personne ou une organisation légitime et offre une sorte de récompense ou présente une situation critique que vous seul pouvez résoudre. Par ex., il peut prétendre être votre banque et exiger des détails de votre compte (informations personnelles, numéros de cartes de crédit, mot de passe, email, etc.) sinon celui-ci sera verrouillé.**
- **Parfois, il vous demande de fournir directement l’information par email. Souvent, il vous demande de cliquer sur le lien vers un site qui est une copie de l’original, pour vous extorquer des informations. Dans ce cas, on parle de « pharming ».**

Exemples de phishing par mail

INFORMATION TECHNOLOGY & SOLUTIONS

- **Un exemple évident!**

Dear Human Greg,

Itz come to our attentionz that you credit card is not update in our database. We has new system that require you to put your infomationz in again. You see, Don spilled a big cup of coffee on the last systemz. I tellz Don, NO YOUZ CANT HAZ COFFEE IN SYSTEM PLACE but he sayz I HAZ COFFEE WHEREVERS. Please, I can haz credit card number? K THX BAI

Sincerely,

Janice, a realz human. (NOT CAT)

Exemples de phishing par mail

INFORMATION TECHNOLOGY & SOLUTIONS

- **Un exemple moins évident de *customerservice@amazon.org***

Dear valued customer,

Your account at <insert your email address> was recently flagged for suspicious activity. Because of this activity, we've temporarily suspended your account and will be permanently deleting it in ten days if you do not verify your information.

To verify your account, please click the link: <malicious link here>. This is an automated message. Please send all replies to accounts@sparklekitten.net.

Sincerely,

Customer Service

Exemples de phishing par mail

INFORMATION TECHNOLOGY & SOLUTIONS

- **Un exemple plus ciblé (*spear phishing*)**

Good morning Karen!

This is Steve from the IT Helpdesk. How's everything in HR today? We are supposed to run updates later tonight on your system but I need to make a few changes from your account before I can do that. Can you send me your account login? I'm really swamped down here and don't have time to walk three floors to your office so I was hoping to remote in real quick. Thanks!

Steve

ABC Company

123 Street

Anywhere, USA

Comment se protéger contre le phishing?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Les e-mails de phishing comportent généralement un sentiment d'urgence ou d'autorité. Si l'e-mail indique que vous devez faire quelque chose immédiatement ou qu'il y aura des conséquences, il y a de fortes chances qu'il s'agisse d'un hameçonnage.**
- **Assurez-vous de vérifier les fautes d'orthographe, les logos d'entreprise incorrects ou les adresses e-mail étranges.**
- **Si vous n'avez jamais utilisé un service, il est très peu probable qu'ils vous envoient un e-mail à l'improviste. Vous n'allez pas recevoir d'argent d'une banque dans laquelle vous n'avez pas de compte.**
- **Le support technique ne vous appellera jamais en premier.**
- **Allez toujours sur le site Web plutôt que de cliquer sur un lien dans un e-mail, sauf si vous êtes absolument sûr de savoir d'où vient l'e-mail.**

Comment le pirate manipule les URLs?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Typosquatting**
  - Les pirates accomplissent le pharming en modifiant le contenu d'une URL ou d'un site Web. Lorsqu'un pirate orthographie mal une URL, cela s'appelle du typosquatting. Par exemple, ils peuvent enregistrer *petmart.com* au lieu de *petsmart.com*. Le DNS recherche ensuite l'URL mal orthographiée au lieu de la vraie et vous envoie vers le site Web dangereux. Aujourd'hui, le typosquattage est un phénomène rare car de nombreuses entreprises enregistrent toutes les fautes d'orthographe possibles du nom de leur site Web pour s'assurer qu'elles accèdent toutes au même site Web authentique.

- **URLs complexes et Redirections**
  - Par exemple, vous pourriez recevoir un e-mail avec un lien qui ressemble à ceci: *ww.accounts.com/user/payments/…* avec les trois points indiquant que le reste de l'URL a été coupé. Bien que cela puisse ressembler à un site Web valide, il pourrait y avoir une partie plus dangereuse à la fin, telle que *payment/files/virus.exe*.
  - Les pirates peuvent également utiliser des redirections pour masquer l'emplacement de leur URL. Une redirection est un morceau de code qui, lorsqu'il est activé, vous renvoie vers un autre site Web au lieu de celui d'origine sur lequel vous avez cliqué.

- **Modifications des enregistrements DNS**
  - Si le pirate peut modifier l'enregistrement DNS, il peut dire à votre navigateur Web d'aller où il veut. Une autre technique de pharming consiste à ajouter des informations au fichier hôte local de votre ordinateur. Un moyen encore plus simple pour les adversaires d'attaquer votre système consiste à modifier l'emplacement de vos requêtes DNS.

Hoaxes (canulars ou infox)

INFORMATION TECHNOLOGY & SOLUTIONS

- Un canular est une histoire inventée créée pour diffuser de fausses informations sur un sujet particulier ; par exemple, sur Internet, il peut s'agir d'une fausse histoire de célébrité ou d'un nouveau remède miracle pour la santé. Les canulars sont initiés pour de nombreuses raisons différentes. Parfois, ils sont conçus simplement comme une blague, comme une ruse sur les nouvelles fonctionnalités du dernier modèle d'iPhone qui n'existent pas réellement.

- Des canulars sont également créés pour endommager ou diffuser des informations trompeuses sur une cible particulière. Par exemple, un pirate pourrait être en colère qu'une certaine entreprise de nourriture pour chats ne fabrique plus la saveur croustillante préférée de son chat. En utilisant de faux rapports de violations du code de la santé, ce pirate pourrait inventer un canular selon lequel la nourriture de l'entreprise est toxique, faisant ainsi hésiter les gens à l'acheter.

- La plupart des canulars sont diffusés via les réseaux sociaux. Une publication ou un article contenant le canular peut rapidement se propager via les publications Facebook ou Twitter. Parfois, de telles tromperies utilisent des informations réelles pour les faire paraître plus légitimes, c'est la raison pour laquelle il peut être difficile d'exposer un canular et de diffuser les bonnes informations. Sans savoir ce qui est vrai, il est difficile de réfuter le canular, surtout s'il vient de quelqu'un en qui vous avez confiance.

Pourquoi les pirates adorent le phishing?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Pas chère, facile, rapide**
- **Et ça marche! Car difficile à contrer!**
  - Les filtres de messagerie ne sont pas infaillibles
  - L'utilisateur ciblé est l'ultime rempart
  - Réfléchissez à 2 fois et ne vous précipitez pas!
    - Aucune société ne vous demandera directement votre mot de passe! Elle peut vous demander de le réinitialiser
    - Aucune société sortie de nulle part ne vous contactera de manière légitime, surtout pour vous offrir des choses gratuitement!?
    - Si on vous demande d'agir tout de suite, arrêtez vous et demandez vous si vous devez vraiment le faire
    - Les sujets juridiques ou pénaux sont rarement traités au téléphone et par email, donc vous ne devez jamais payer une taxe ou une amende sans vérifier d'abord, en personne si possible, qu'il s'agit bien d'une demande officielle.

Prenez une route alternative!

INFORMATION TECHNOLOGY & SOLUTIONS

- Même si vous prenez des précautions, il peut être difficile de reconnaître quand quelqu'un essaie de vous arnaquer, surtout s'il déploie des tactiques de spear phishing. **Mais gardez à l'esprit que vous avez toujours la possibilité d'utiliser un autre itinéraire pour vérifier si quelque chose se passe bien.** Par exemple, disons que quelqu'un prétendant être de votre banque appelle et dit qu'il y a un problème avec votre compte. **Au lieu de vous en occuper tout de suite, dites-leur que vous êtes occupé et que vous rappellerez plus tard pour résoudre le problème.** Les pirates détestent quand cela se produit parce qu'ils savent que vous ne les rappellerez pas mais que vous appellerez à la place la vraie banque.

- Vous pouvez utiliser cette tactique pour n'importe quelle méthode de phishing. **Au lieu de cliquer sur un lien qui vous a été envoyé dans un e-mail, vous pouvez accéder au site Web en effectuant une recherche sur Google ou en tapant directement son URL**. En fait, vous ne devriez jamais cliquer sur un lien dans un e-mail à moins d'être absolument sûr d'où vient l'e-mail. **Vous pouvez également utiliser des serveurs DNS bien connus pour vous assurer que vous accédez au site réel.** Changer votre navigateur pour utiliser le serveur DNS 8.8.8.8 (DNS de Google) ou 1.1.1.1 (DNS sécurisé de Cloudflare) est un bon moyen d'éviter le piratage DNS.

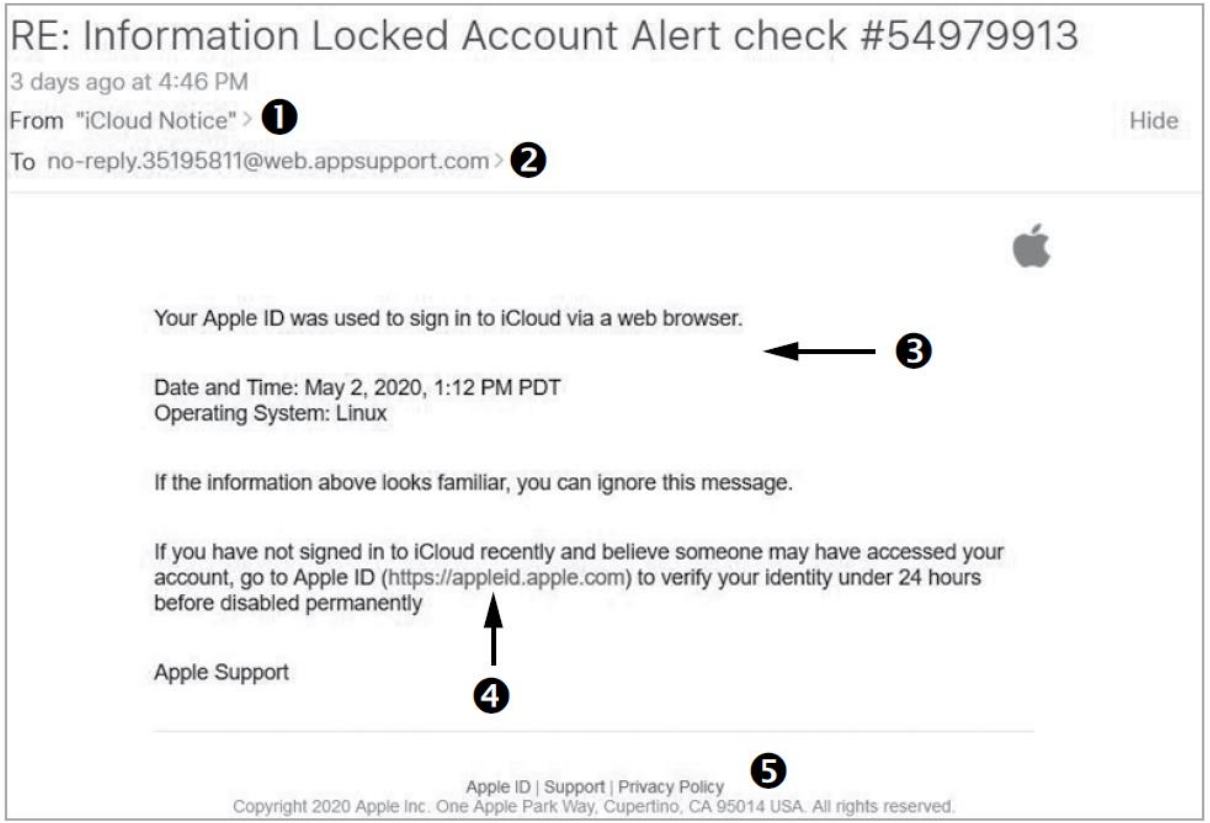
Fiez vous à votre bon sens!

INFORMATION TECHNOLOGY & SOLUTIONS

- **N'oubliez jamais que vous êtes la meilleure ligne de défense contre les tentatives de phishing.**
- **Si vous voyez quelque chose de suspect, écoutez votre voix intérieure et faites des recherches pour déterminer si c'est légitime. C'est aussi à vous d'en alerter les autres.**
- **Vérifier si une source est digne de confiance prend plus de temps, mais cela aide à empêcher les fausses rumeurs de se répandre sur Internet.**

Exercice: Analyser un email de phishing

INFORMATION TECHNOLOGY & SOLUTIONS



Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Qu’est-ce qu’un Malware?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Les logiciels malveillants sont des logiciels conçus pour endommager les systèmes informatiques. Ainsi, même si un jeu peut consommer toute la mémoire de votre ordinateur, il n'est pas considéré comme un logiciel malveillant.**

- **La meilleure façon de définir les dommages causés par les logiciels malveillants est les dommages causés par une action non autorisée considérée comme anormale pour le système. Par exemple, une opération normale peut impliquer un utilisateur se connectant au système à l'aide d’un nom d'utilisateur et mot de passe configurés par un administrateur interne. Si une application permet à un pirate d'accéder au système sans utiliser de nom d'utilisateur et de mot de passe, il a effectué une action non autorisée.**

Types de Malware

INFORMATION TECHNOLOGY & SOLUTIONS

- **Virus**
- **Vers (Worms)**
- **Troyens (Trojans)**
- **Rançongiciels (Ransomware)**
- **Spyware et Adware**
- **Rootkits et Bootkits**
- **Malware polymorphique**

Diffusion des Malwares par les pirates

INFORMATION TECHNOLOGY & SOLUTIONS

- La première étape de tout déploiement de malware consiste à **créer le logiciel destructeur**. Généralement, les adversaires le font de deux manières : en profitant d'une vulnérabilité existante ou en repartant de zéro. De nombreux pirates utilisent des logiciels malveillants déjà conçus pour exploiter une vulnérabilité pour leurs propres attaques.

- Après avoir créé le code destructeur, l'attaquant passe à l'étape suivante : **l'infection initiale**. Ils peuvent installer le logiciel nuisible sur un système par divers moyens, mais le plus efficace est **l'ingénierie sociale**. En utilisant des **techniques de phishing**, il est souvent facile d'amener les utilisateurs à télécharger le malware et à l'exécuter.

- **L'infection initiale libérera la pleine charge utile**, mais cela ne signifie pas que le malware a nécessairement fini de fonctionner. À ce stade, certains logiciels malveillants se concentrent sur une action spécifique ; par exemple, un ransomware crypte des fichiers ou d'autres supports de stockage. D'autres malwares se concentrent sur la **création d'un APT**, qui est un malware sophistiqué qui reste caché sur un réseau pendant une longue période, recueillant des données et d'autres informations avant d'exécuter une attaque de grande envergure.

- Une fois l'infection en place et la charge utile déployée, **la contagion peut se propager**. Cela peut impliquer l'envoi du logiciel malveillant dans un e-mail à l'aide de la liste de contacts du système hôte ; se déplacer sur le réseau à l'aide de protocoles de transport, tels que le protocole de transfert de fichiers (FTP) ou le protocole de transfert hypertexte (HTTP) ; ou se cacher dans un fichier jusqu'à ce qu'un nouvel utilisateur clique dessus.

Se protéger contre les Malwares

- La meilleure façon de se défendre contre les logiciels malveillants est **d'utiliser des logiciels anti-malware, communément appelés programmes antivirus** (bien qu'ils protègent désormais contre presque toutes les formes de logiciels malveillants, pas seulement les virus). Les programmes antivirus sont disponibles auprès de nombreux fournisseurs commerciaux. Les systèmes Microsoft disposent également d'un programme antivirus intégré appelé Microsoft Defender (anciennement Windows Defender).

- Les logiciels antivirus se présentent sous **deux formes de détection de base : signature et heuristique**. Le premier utilise une signature de code pour reconnaître les logiciels malveillants. **Une signature de code est une partie unique du code** d'un malware qui permet de l'identifier. Le logiciel antivirus de signature est extrêmement rapide car il ne fait que comparer un morceau de code à une base de données de signatures pour vérifier s'il s'agit d'un logiciel malveillant. **La détection antivirus heuristique adapte sa détection en fonction du flux de trafic sur un réseau**, à la recherche d'anomalies en dehors du flux de trafic normal. Ce qui est normal varie en fonction de la façon dont le réseau est utilisé, de sorte que le programme antivirus heuristique doit passer du temps à apprendre cette ligne de base. Il peut alors constater des anomalies.

Exercice*: Analyser un Malware

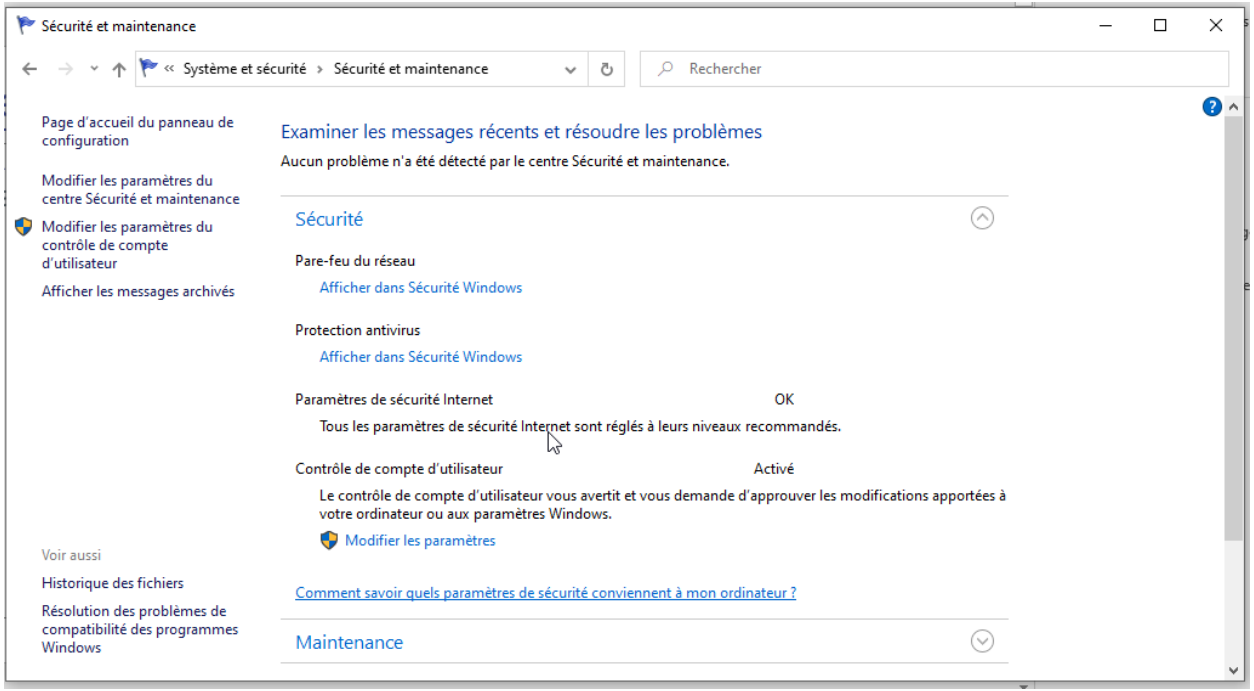
INFORMATION TECHNOLOGY & SOLUTIONS

- **Objectif: Utiliser un outil gratuit en ligne pour scanner un fichier PDF et vérifier s'il est infecté par un malware ou pas.**
- **Pour effectuer cet exercice, vous pouvez utiliser un document PDF:**
  - Ne poster pas de fichier contenant des informations personnelles!!!
- **Accéder au site d'analyse en ligne VirusTotal et télécharger le fichier suspicieux:**
  - https://www.virustotal.com/gui/home/upload
- **Accéder au site d'analyse en ligne Joe Sandbox et télécharger le fichier suspicieux:**
  - https://www.joesandbox.com
- **Analyser et comparer les résultats**

Exercice*: Paramétrer un antivirus

INFORMATION TECHNOLOGY & SOLUTIONS

- **Sous Windows 10**
  - Panneau de configuration\Système et sécurité\Sécurité et maintenance



Exercice*: Paramétrer un antivirus

INFORMATION TECHNOLOGY & SOLUTIONS

- **Dans « Protection antivirus »**
  - **Scan Options**
    - Quick scan
    - Full scan
    - Custom scan
    - Windows Defender Offline scan
  - **Protection History**
    - Détection des menaces et mise en quarantaine
  - **Real-time Protection**
    - Base de signatures antivirales à jour / ressources heuristiques en ligne
  - **Ransomware Protection**
    - Sauvegardes en ligne automatiques de certains fichiers
    - Cela ne dispense pas de sauvegardes régulières sur des disques externes ou dans le cloud

Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Authentification

INFORMATION TECHNOLOGY & SOLUTIONS

- **L'authentification consiste à vérifier que la personne est bien ce qu'elle prétend être.**

- **Types d'authentification**
  1. Quelque chose que vous connaissez (ex. mot de passe)
  2. Quelque chose que vous possédez (ex. carte à puce, certificat numérique)
  3. Quelque chose que vous êtes (ex. attribut biométrique)
  4. Quelque chose que vous faites (ex. CAPTCHA = "Completely Automated Public Turing test to tell Computers and Humans Apart")
  5. Quelque part où vous êtes (localisation)

- **Authentification multi-facteurs**
  - Une combinaison de plusieurs types d'authentification
    - Ex: Login/Password + code de vérification via email or SMS (bientôt obsolète pour les banques en ligne)

Autorisation

INFORMATION TECHNOLOGY & SOLUTIONS

- **Une fois l'utilisateur authentifié, il doit être autorisé à effectuer certaines actions (contrôle d'accès).**

- **Les 5 schémas communs de contrôle d'accès:**
  1. Contrôle d'accès strict (cf. classification des documents militaires)
  2. Contrôle d'accès basé sur une règle (ex. permissions fichiers)
  3. Contrôle d'accès basé sur un rôle (ex. responsable RH) ou RBAC
     - Concept du moindre privilège (least privilege)
     - Séparation des responsabilités (separation of duties)
  4. Contrôle d'accès basé sur un attribut ou ABAC
     - Similaire à RBAC mais avec la restriction de l'attribut (= mini-rôle)
     - Ex: attribut recruteur + attribut RH
  5. Contrôle d'accès à discrétion ou DAC
     - Ex. services documentaires (OneDrive ou Google Drive)

Accounting (ou comptabilité)

INFORMATION TECHNOLOGY & SOLUTIONS

- **L'accounting consiste à s'assurer que chaque action effectuée sur un système ou un réseau génère un enregistrement.**

- **L'accounting est d'importance vitale pour maintenir la sécurité d'une organisation. Si vous n'êtes pas capable de vérifier l'activité concernant un compte ou un système à un instant donné, vous ne serez pas en mesure de savoir si la sécurité est maintenue. De plus si un incident arrive, il sera très difficile d'obtenir les détails de l'attaque et de repousser l'adversaire hors de l'environnement.**

- **Par conséquent, Il est donc important de maintenir l'accounting à l'aide d'un double processus :**
  1. Activation de la journalisation
  2. Exécution de la routine d'audit.

Journalisation (Syslog)

INFORMATION TECHNOLOGY & SOLUTIONS

- **Niveaux de sévérité des logs**

Value	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but requires special handling.
6	Informational	Informational messages.
7	Debug	Debugging messages.

Audit

INFORMATION TECHNOLOGY & SOLUTIONS

- **Vous devez effectuer des audits non seulement pour détecter les activités malveillantes, mais également pour la routine de maintenance.**
- **Pour que l'audit fonctionne, vous ne pouvez pas le faire uniquement lorsque vous avez un problème. Vous devez détecter les problèmes dès qu'ils surviennent, avant qu'un matériel, une panne, un bug logiciel ou une compromission, ne causent des dommages importants à vos systèmes.**
- **Chaque événement sur un système doit produire un log. Décider combien de ces logs vous devez auditer peut être un sujet délicat. Si vous auditez trop, vous perdrez du temps à parcourir des événements normaux. Si vous auditez pas assez, vous manquerez des indicateurs clés d'activité malveillante.**
- **Pour mieux traquer les attaques de type APT, vous pouvez utiliser un système de gestion de l'information et des événements (SIEM). Le SIEM va corréler les logs de tous les appareils et réseaux de votre organisation pour identifier des comportements suspicieux.**

Indicateurs d'Attaques (IoAs) #1

INFORMATION TECHNOLOGY & SOLUTIONS

IoA	Example	Possible activity
Unusual outbound traffic	Device connecting to known malicious IP address; device using unusual protocols, like FTP; large amount of queries to a particular website or group of websites	Malware contacting a command-and-control server; files being removed; backdoor being accessed
Internal device running network scans	Workstation or server sending out ping packets	Malware or black hat looking for other systems to compromise
Account login from location outside business area	Logins from foreign countries; logins from multiple different locations at the same time	Compromise of account credentials by black hat or botnet
Changes to system settings	Firewall changes or port changes to allow new traffic to connect, such as opening FTP ports; new accounts added to the system; an account given administrator access; new automated tasks created	Compromise of system by malware or black hat
Changes to email settings	New inbox rules created; new mail flow rules; dramatic increase in email activity from an account	Compromise of email account; use of email to send out spam or phishing attacks

Indicateurs d'Attaques (IoAs) #2

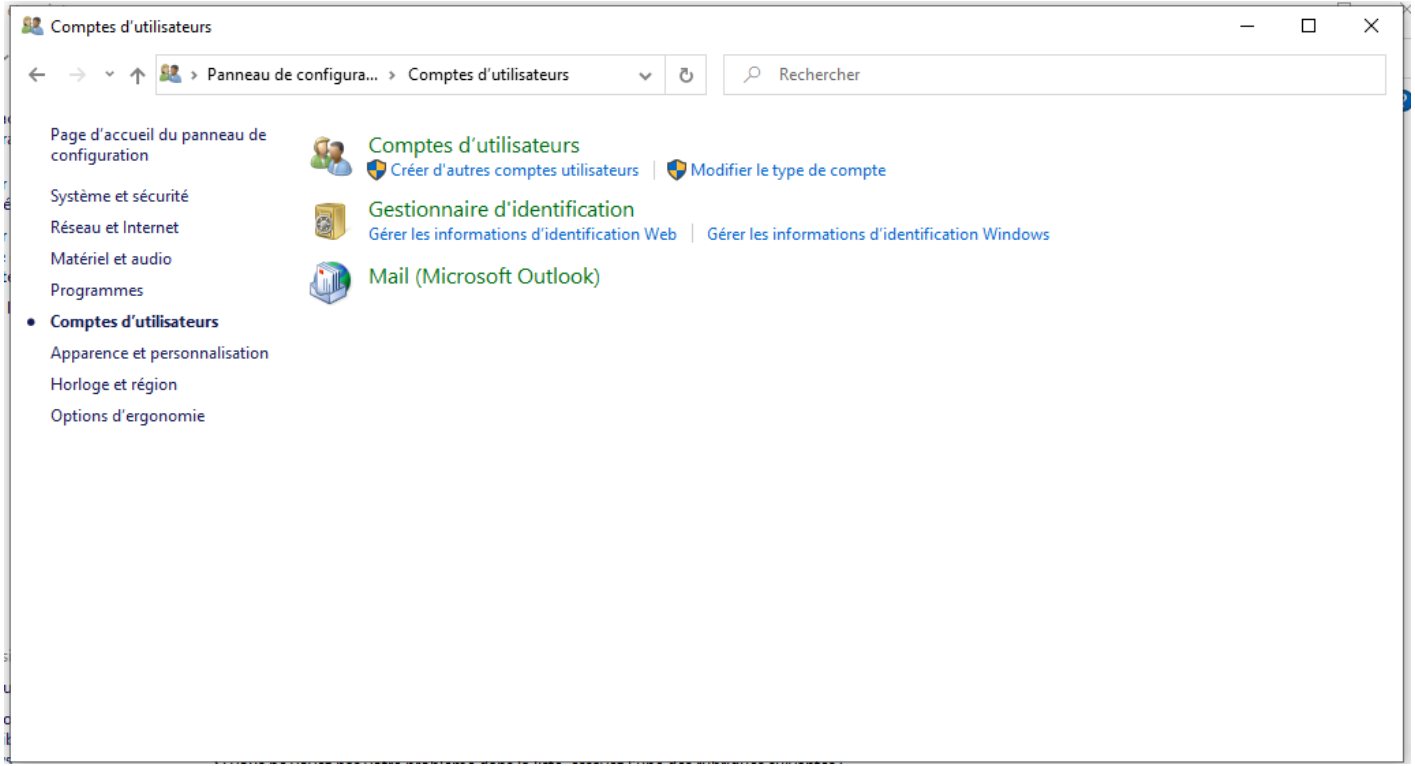
INFORMATION TECHNOLOGY & SOLUTIONS

Application or system making irregular connections	System in an external network connecting to an internal system; application making new or unusual requests, such as trying to download data from a read-only database; system attempting to access a device it's not authorized to or that is outside its normal workflow (for example, a front desk workstation trying to connect to an HR database)	Compromise of application or system by malware or black hat; attacker then uses compromise to attempt to steal data from, or gain access to, other systems on the network
Multiple rapid failures	Several failed login attempts; multiple access request failures; multiple system failures	Black hat is attempting to access a system or account, for example, using a brute-force attack on an account login; might be trying to use system failures to bypass normal security controls
Unauthorized programs or processes running	Programs are set to run on startup and aren't part of normal business software; processes consume a lot of memory or CPU resources	Malware, particularly a trojan
Activity outside of normal operation time	Website queries, emails sent, applications run, or logins made during non-business hours	Compromise of system by malware or black hat, including possible backdoor or trojan

Exercice: Configurer des comptes

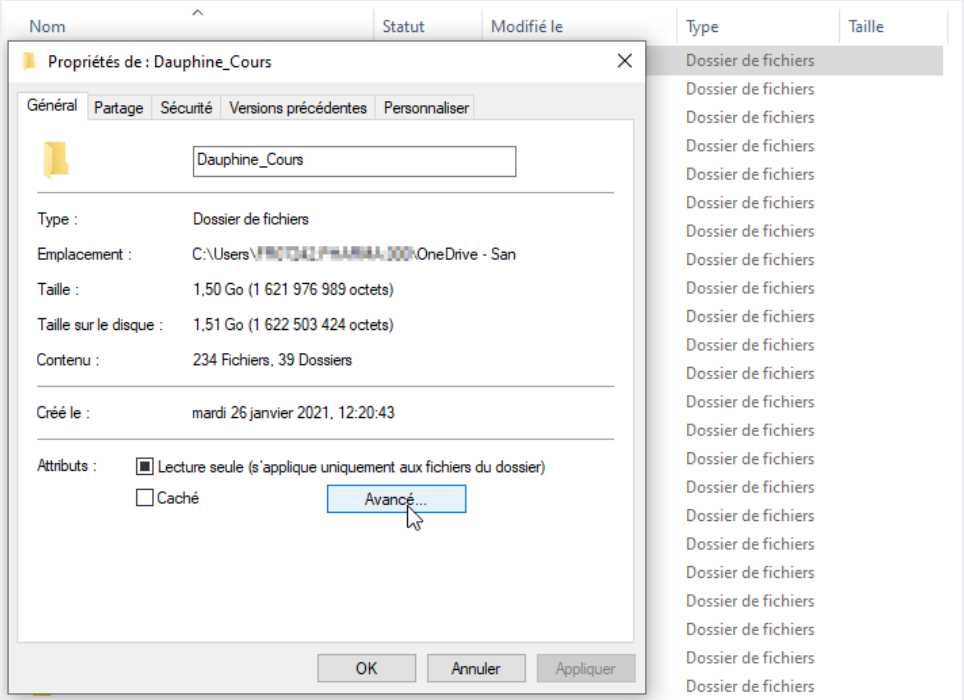
INFORMATION TECHNOLOGY & SOLUTIONS

- **Sous Windows 10:**



Exercice: Partager un dossier

- **Sous Windows 10**:



Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Comment les pirates observent votre trafic?

INFORMATION TECHNOLOGY & SOLUTIONS

- **Sur les réseaux câblés, les pirates peuvent intercepter le trafic (sniffing) en utilisant différentes techniques:**
  - Par l'ajout de matériel sur le réseau (**network tap**). L'équipement peut scanner et copier le trafic qui circule sur le réseau.
  - Un adversaire peut également utiliser une technique appelée usurpation d'adresse IP (**IP Spoofing**) par laquelle il copie l'adresse IP d'un appareil légitime sur le réseau et imite cet appareil.
  - Une troisième méthode consiste à changer l'endroit où le trafic est envoyé en modifiant les paramètres réseau. Par exemple, en modifiant la passerelle par défaut (**default gateway**) sur un appareil, un pirate peut décider où va le trafic quittant le réseau. Un adversaire peut également activer la mise en miroir des ports (**port mirroring**) sur un commutateur.
  - Une autre méthode qu'un attaquant peut utiliser consiste à exploiter physiquement le câble par lequel le trafic passe (**prise vampire**)

Prise vampire

INFORMATION TECHNOLOGY & SOLUTIONS

Attaque Man-in-the-Middle

INFORMATION TECHNOLOGY & SOLUTIONS

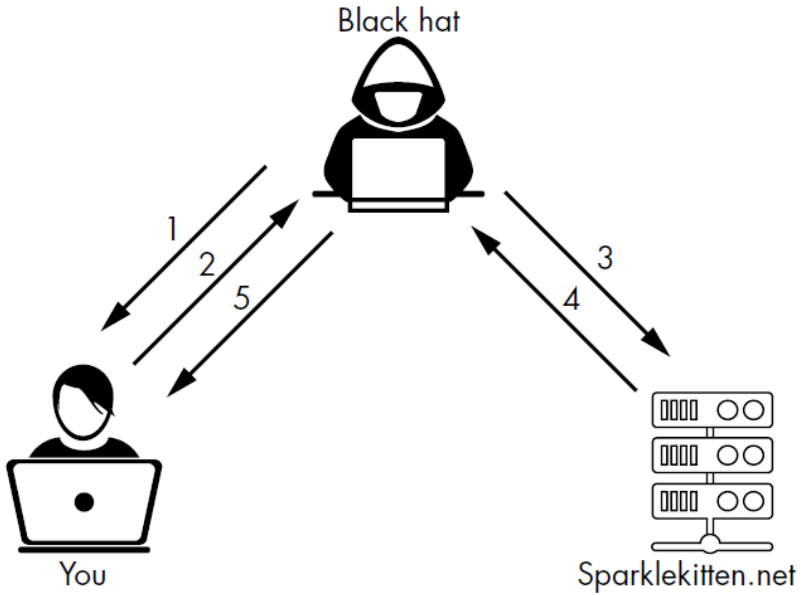
Dans ce scénario, 1) le pirate vous envoie un e-mail de phishing avec ce qui semble être un lien légitime de votre banque. Lorsque vous cliquez sur le lien dans l'e-mail, il vous dirige vers le faux serveur Web, où il a créé une page qui ressemble au site Web de votre banque.

2) Vous entrez ensuite vos informations d'identification sur ce site Web. L'adversaire reçoit le trafic que vous envoyez au site Web et le modifie pour qu'il semble provenir de l'ordinateur de l'attaquant plutôt que du vôtre.

3) L'attaquant l'envoie ensuite au site bancaire légitime

4) Il accède à votre compte

5) L'attaquant vous envoie ensuite une erreur 404 Not Found, vous ne réaliserez donc pas ce qui s'est passé.

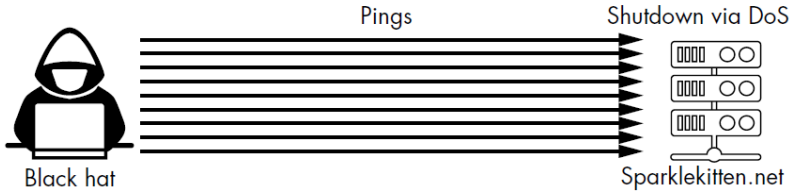


Déni de Service (DoS)

L’attaque par inondation de Ping (Ping flood)

- Dans une **attaque par inondation de ping**, l'appareil d'un adversaire envoie tellement de pings par seconde que l'appareil cible est incapable de communiquer sur le réseau. Les paquets ping peuvent remplir la mémoire du système et le ralentir. Les inondations de ping sont faciles à exécuter, car elles nécessitent simplement un système capable d'envoyer des pings et ayant plus de bande passante que le système cible.

- Une autre forme d'attaque DoS exploite des bogues dans le code pour provoquer un état DoS. Un exemple est connu sous le nom de **ping de la mort**. Les paquets ping ont généralement une taille maximale de 65 535 bits, mais il est possible de créer un paquet ping plus grand que cette limite. Si un pirate peut envoyer un paquet ping plus volumineux à un périphérique, cela peut entraîner le crash et l'arrêt du système recevant le ping.



Déni de Service Distribué (DDoS)

INFORMATION TECHNOLOGY & SOLUTIONS

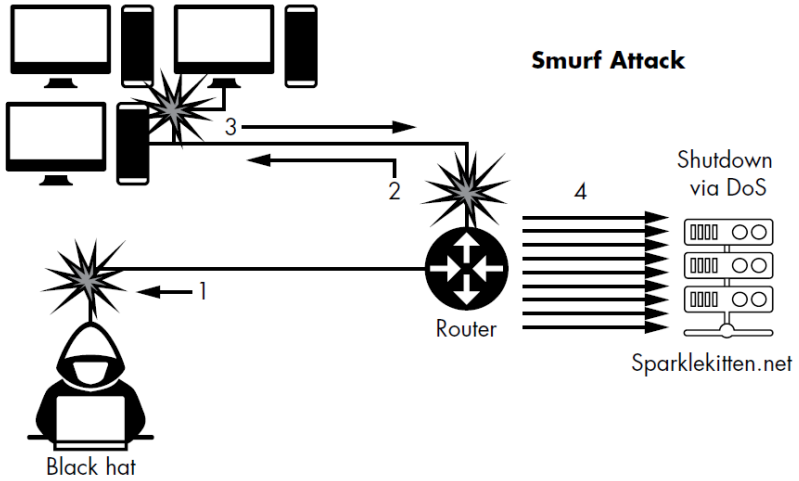
Attaque Smurf

Après avoir usurpé l'adresse IP, 1) l'attaquant envoie un ping à une adresse de diffusion sur un grand réseau.

2) Les adresses de diffusion envoient automatiquement le trafic à tous les autres appareils du réseau.

3) Le ping a été envoyé à tous les appareils du réseau individuellement. Ils ont ensuite répondu à l'adresse IP de la cible .

4) La cible a été submergée de réponses et se crashe.



Déni de Service Distribué (DDoS)

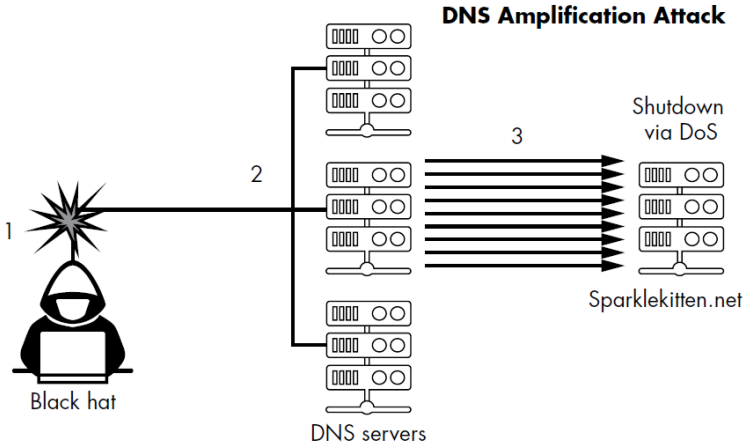
INFORMATION TECHNOLOGY & SOLUTIONS

Attaque par amplification DNS

Semblable à l'attaque Smurf, l'attaque d'amplification DNS utilise des requêtes DNS de base pour submerger la connexion d'une victime à Internet. 1) Le pirate élabore des requêtes DNS qui usurpent l'adresse IP de la victime.

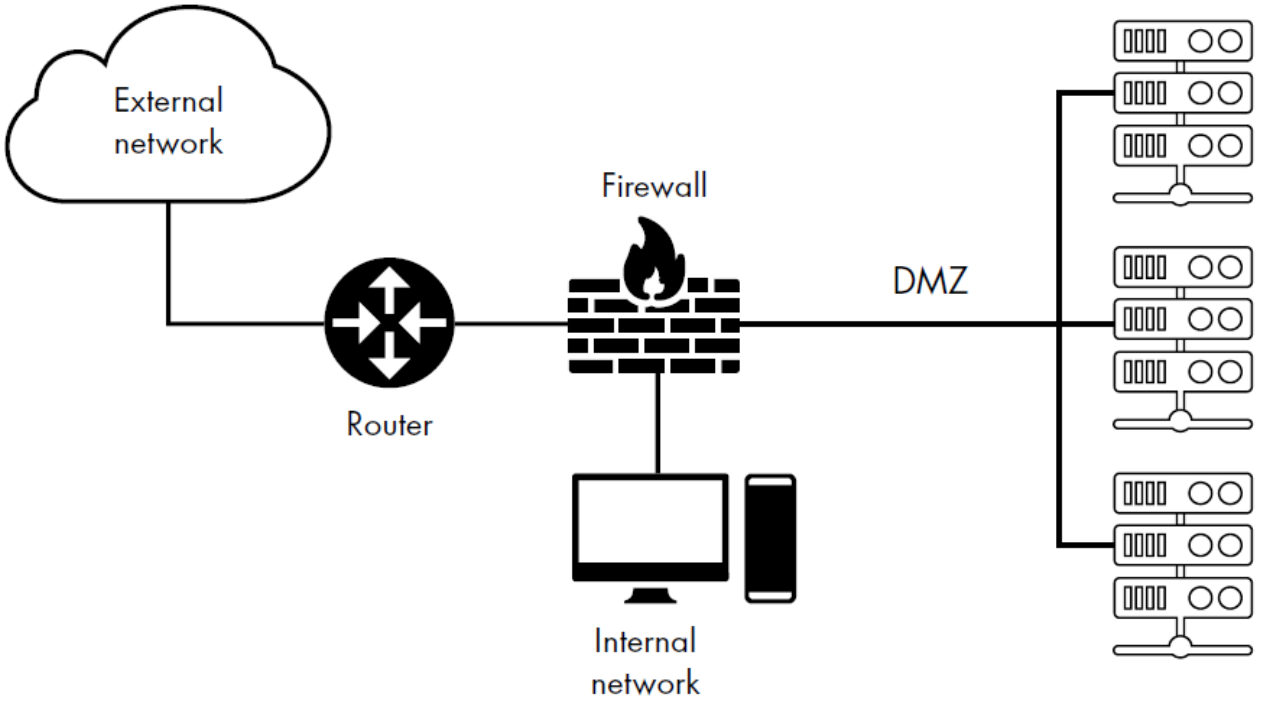
2) Ces requêtes incluent également des paramètres de réponse volumineuse, ce qui signifie qu'elles accepteront la plus grande taille possible d'une réponse à une seule requête. L'adversaire envoie ensuite un flux constant de ces requêtes aux serveurs DNS accessibles au public.

3) Bien que les requêtes soient relativement petites, les réponses sont importantes. Les serveurs DNS envoient ces réponses volumineuses à l'adresse IP de la victime, provoquant un état de DoS.



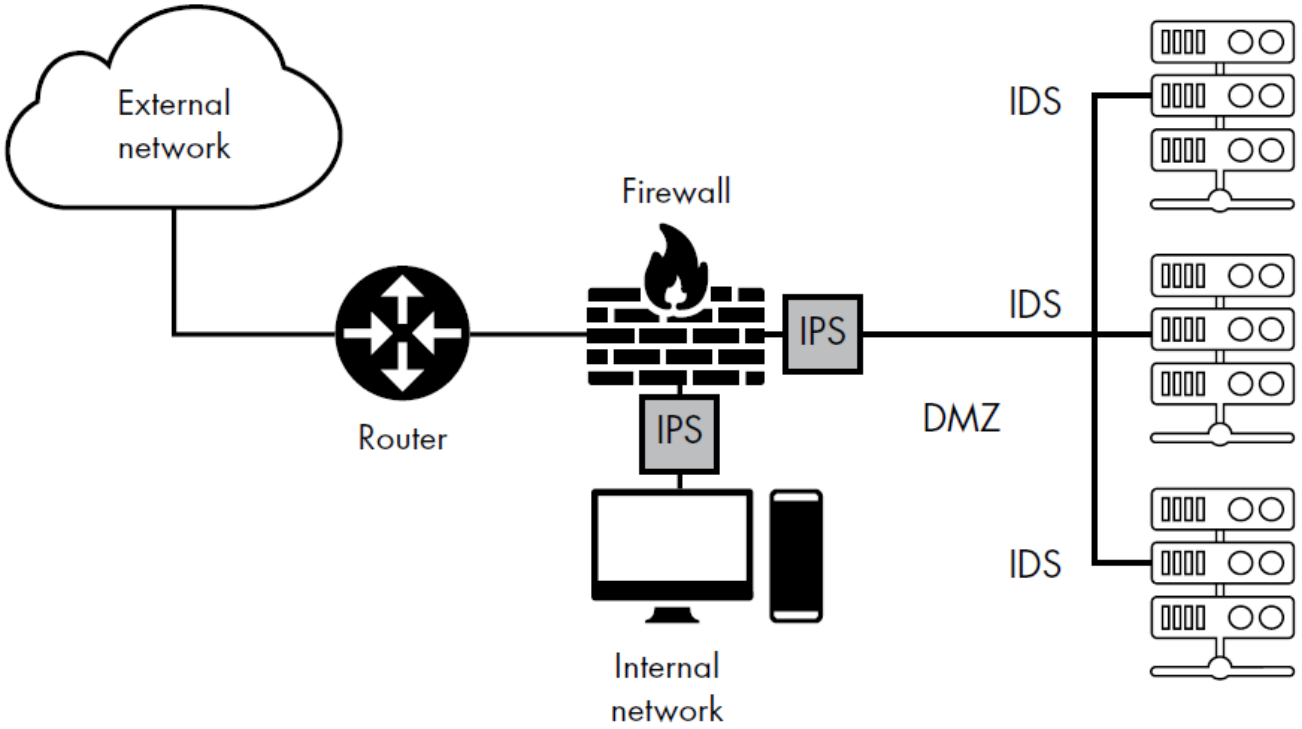
La défense contre les attaques réseau

Les zones démilitarisées (DMZ)



La défense contre les attaques réseau

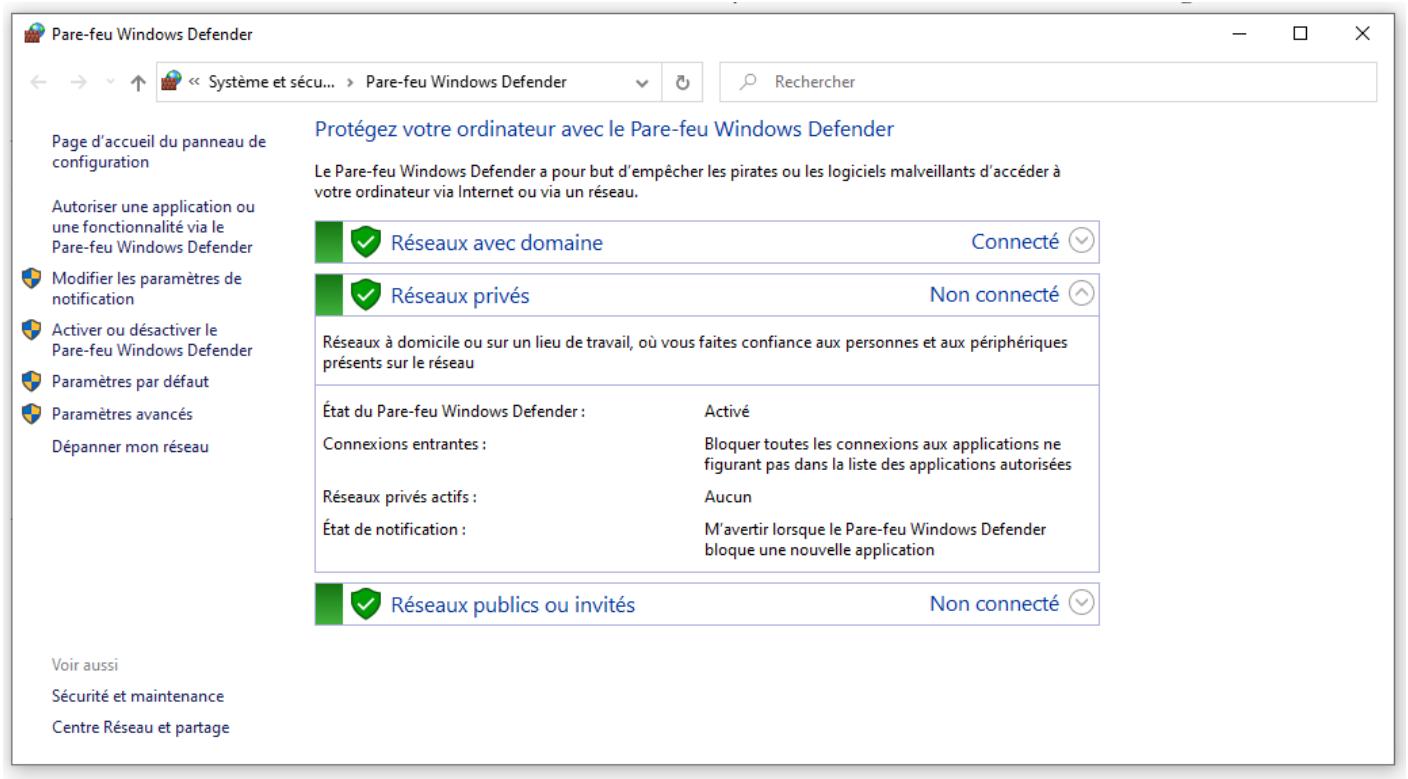
Les Firewalls, IDS et IPS



Exercice: Paramétrer votre Firewall

INFORMATION TECHNOLOGY & SOLUTIONS

- **Sous Windows 10:**



Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Cloud Computing

INFORMATION TECHNOLOGY & SOLUTIONS

Software as a Service (SaaS)	Office 365 Salesforce Electronic medial record applications
Platform as a Service (PaaS)	Squarespace Gmail OneDrive
Infrastructure as a Service (IaaS)	Amazon Web Services Microsoft Azure Google Cloud Services

Attaques du Cloud

INFORMATION TECHNOLOGY & SOLUTIONS

- **Social engineering et les attaques sur l'authentification**
  - Ex: Compte Gmail ou Office 365
- **Attaque Man-in-the-Middle**
  - Ex: Fausse page imitant la page de login du service Cloud
- **Attaque via Malware**
  - Ex: Crypto-mining malware
- **Attaques des applications Web**
  - Exécution de code arbitraire
    - Dépassement de tampon (Buffer Overflows)
    - Injection SQL
    - Injection XML

Défenses du Cloud

INFORMATION TECHNOLOGY & SOLUTIONS

- **Les services cloud sont souvent plus sécurisés que les systèmes que vous possédez et exécutez en propre. La raison en est que les fournisseurs de cloud peuvent dépenser plus d'argent en sécurité que les petites entreprises.**

- **Avant de vous inscrire à un service cloud, examinez attentivement ses conditions d'utilisation pour déterminer le niveau de sécurité que le fournisseur de cloud maintiendra. Les conditions doivent également vous indiquer ce dont vous, en tant que client, êtes responsable. De nombreux fournisseurs de cloud conservent des rapports de conformité, tels qu'un rapport SOC II, que vous pouvez demander.**

- **L'un des points les plus faibles de la sécurité du cloud réside dans les portails clients accessibles au public. La plupart des attaques décrites jusqu'à présent commencent sur la page Web que le client utilise pour interagir avec le service cloud. L'utilisation de l'authentification multifacteur peut également protéger le service cloud. De nombreux attaquants abandonneront et passeront à des victimes plus faciles plutôt que de prendre le temps de percer l'authentification multifacteur.**

- **La surveillance de l'accès de votre service cloud à d'autres applications, systèmes ou comptes peut vous aider à vous assurer qu'un pirate n'a pas pris le contrôle de votre compte cloud ou utilisé le service cloud pour accéder à vos systèmes internes.**

Exercice: Réaliser une injection SQL

INFORMATION TECHNOLOGY & SOLUTIONS

Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Standards sans-fil (IEEE 802.11)

INFORMATION TECHNOLOGY & SOLUTIONS

Standard	Signal type	Max range	Speed
802.11a	5 GHz	120 m	54 Mbps (megabits/second)
802.11b	2.4 GHz	140 m	11 Mbps
802.11g	2.4 GHz	140 m	54 Mbps
802.11n	2.4/5 GHz	250 m	600 Mbps
802.11ac	5 GHz	120 m	3466 Mbps (3.4 Gbps)
802.11ax	2.4/5/6 GHz	120 m	9608 Mb/s (9.6 Gbps)

Sécurité sans-fil

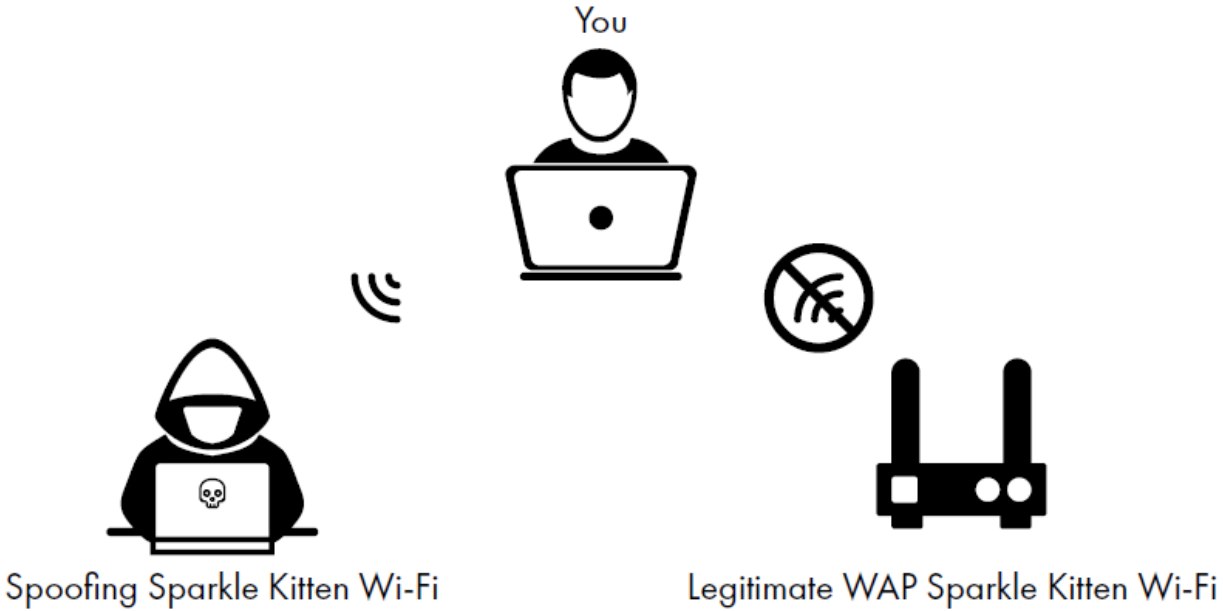
INFORMATION TECHNOLOGY & SOLUTIONS

- **Authentification**
  - Personal ou mode PSK (pre-shared key)
  - Mode Enterprise utilisant le protocole EAP (Extensible Authentication Protocol) ou 802.1X

- **Chiffrement**
  - Wired Equivalent Privacy (WEP) – obsolète
  - Wi-Fi Protected Access (WPA) utilisant le protocole TKIP (Temporal Key Integrity Protocol)
  - WPA2 utilisant AES (Advanced Encryption Standard) – il inclut le 802.1X

Attaques des réseaux sans fil

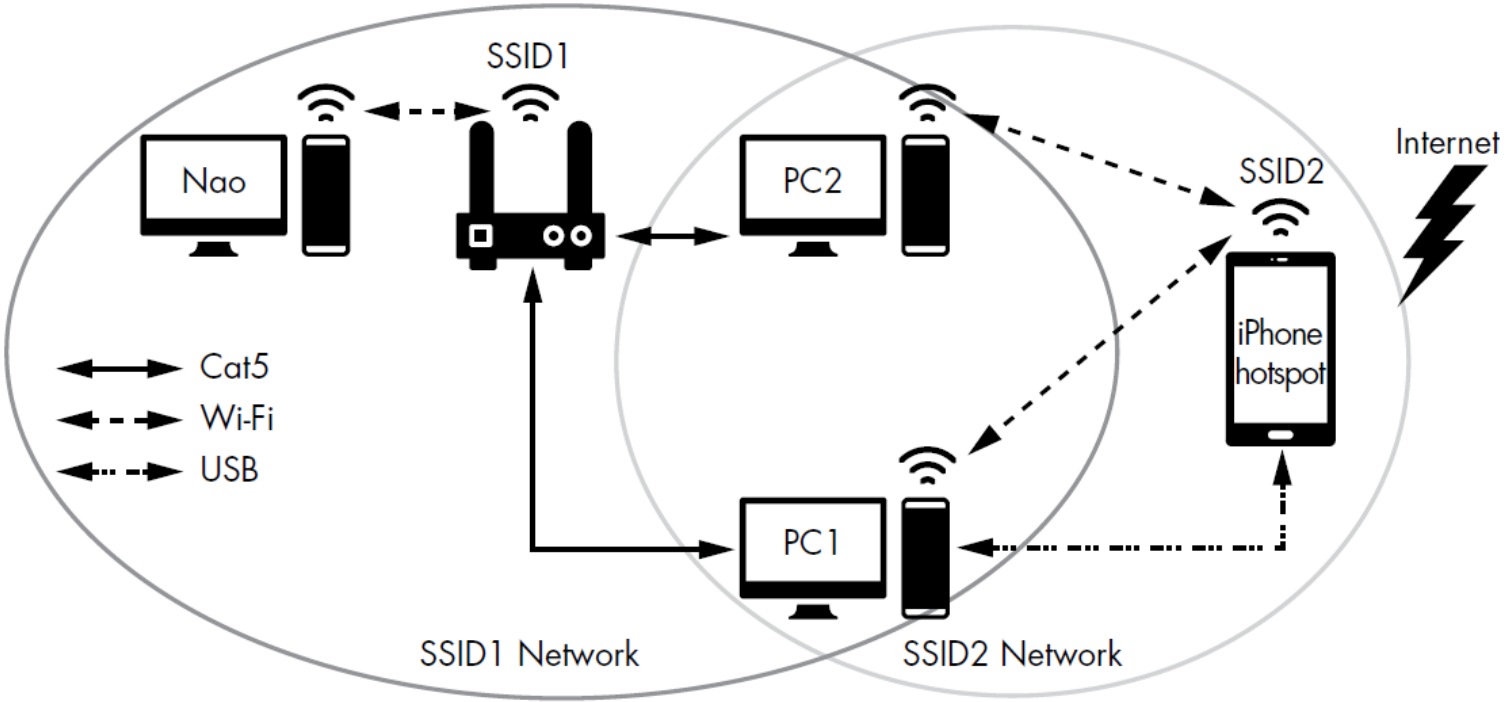
- **Points d'accès pirate (Rogue Access Point)**
  - Attaque Evil Twin



Configurer un réseau sans fil

INFORMATION TECHNOLOGY & SOLUTIONS

- **Créer un diagramme du réseau sans fil**



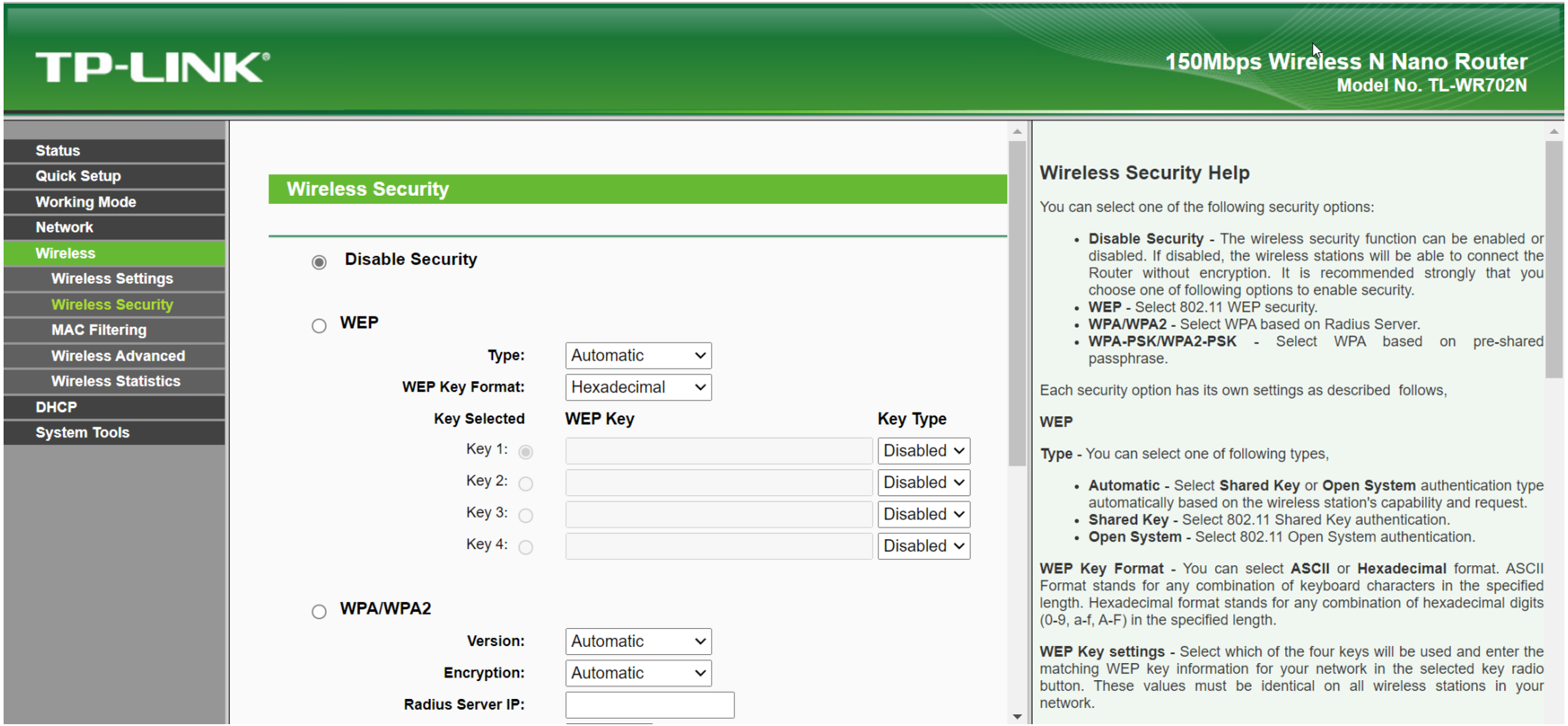
Configurer un réseau sans fil

INFORMATION TECHNOLOGY & SOLUTIONS

- **Vérifier que les points d'accès utilisent WPA2 pour le chiffrement, soit l'authentification 802.1X ou une clé robuste.**
- **S'assurer que les WAPs sont segmentés avec leur propre sous-réseau sur le réseau interne (cf. DMZ)**
- **Effectuer une enquête du site (site survey) régulièrement pour identifier d'éventuels points d'accès pirate ou des SSIDs cachés.**
- **Les réseaux sans fil exigent plus de sécurité et de vigilance que les réseaux câblés, car il est plus facile de capter un signal sans fil.**
- **Dans la mesure du possible, éviter d'envoyer des données sensibles sur un réseau sans fil sans les chiffrer au préalable.**
- **Eviter d'utiliser des réseaux sans fil publics (café, aéroport, etc.) et toujours vérifier que vous utilisez au moins le chiffrement WPA2.**

Exercice*: Sécuriser votre point d'accès

INFORMATION TECHNOLOGY & SOLUTIONS



Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

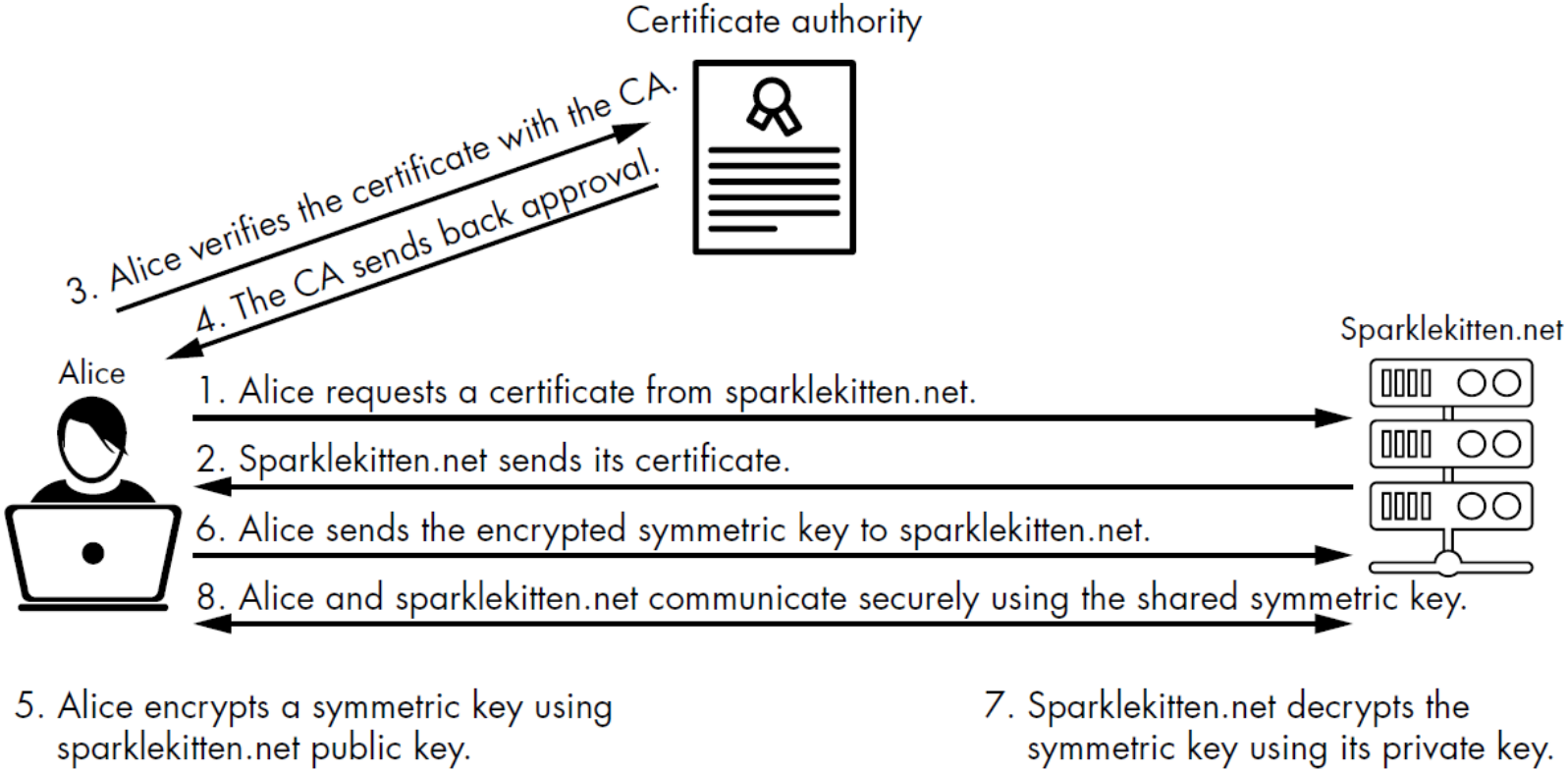
1. **Notions de base**
2. **Cibles d'attaques sur Internet**
3. **Tactiques de phishing**
4. **Infections par malwares**
5. **Vols de mots de passe et contrôle d'accès**
6. **Attaques réseau**
7. **Attaques du Cloud**
8. **Piratage du réseau sans fil**
9. **Casser le chiffrement**
10. **Analyse de risques**

Cryptologie moderne

INFORMATION TECHNOLOGY & SOLUTIONS

- **Algorithmes symétriques**
  - DES (Data Encryption Standard), clé à 56 bits
  - 3DES, clé à 168 ou 112 bits
  - AES (Advanced Encryption Standard) 256 bits
- **Algorithmes asymétriques**
  - RSA (Rivest Shamir Adleman) 2048 bits
- **Certificats numériques**
  - Autorité de Certification (CA) et Infrastructure de clés publiques (PKI)
- **Hachage**
  - MD5 (Message Digest 5), 128 bits
  - SHA (Secure Hashing Algorithm)
    - SHA-1, 160 bits
    - SHA-2, 256 bits
    - SHA-3, 512 bits

Accès à un site web sécurisé



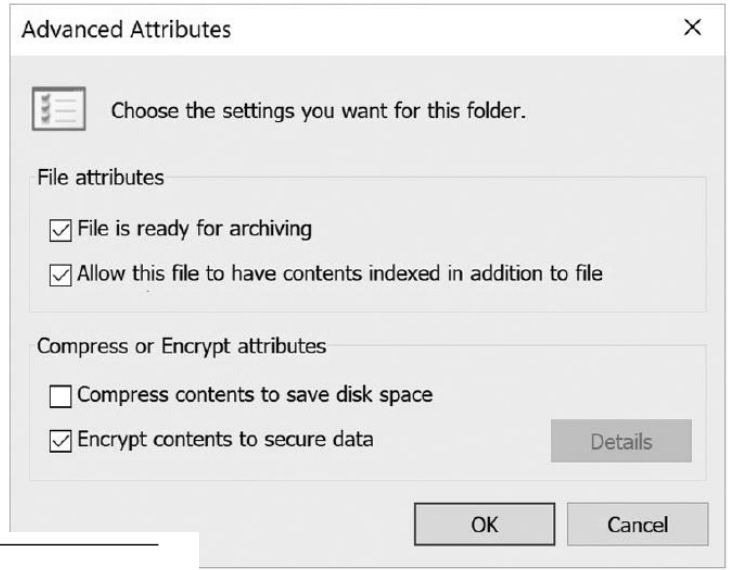
Exercice: Chiffrer et hâcher des fichiers

INFORMATION TECHNOLOGY & SOLUTIONS

- **Sous Windows 10 (Version Pro):**

```
C:\Windows\System32> certutil -hashfile C:\Users\SparkleKitten\Documents\
Secretfile.txt SHA512

SHA512 hash of C:\Users\samgr\Desktop\Secret\SuperSecret.txt:
0dd47a4aa75835dfd19b1bb6ed5f8f60cc87492dacf8284ef598229cc258244f67d430e18d7c
770d36ed8b205af1571f42f9956bbe544a362ca191256450eb0
CertUtil: -hashfile command completed successfully.
```



- **Sous MacOS**

```
$ shasum ~/Documents/Secret.rtf

2966acd0faf387e024b8b6be50f47450c3c2f7fb  /Users/sparklekitten/Documents/
Secret.rtf
```

Exercice*: Générer une clé publique

INFORMATION TECHNOLOGY & SOLUTIONS

- **Sous Windows 10:**

```
C:\Windows\System32> ssh-keygen

Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\samgr/.ssh/id_rsa): mykey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in mykey.
Your public key has been saved in mykey.pub.
The key fingerprint is:
SHA256:FCRaZDnraock8vueS1FqjEZmdzcRB+LqXzRvRwqrLxc samgr@DESKTOP-OPFVANO
The key's randomart image is:
+---[RSA 2048]----+
|     .*o*o.      |
|     =oo +       |
|  + o +o+        |
| + + =.o .       |
|  o *.  S   .    |
|...o....E= o     |
| o ooo  o.+ .    |
|  ..+ooo.. .     |
|  .==oo+.        |
+----[SHA256]-----+
```

Cybersécurité - Compléments et Exercices

INFORMATION TECHNOLOGY & SOLUTIONS

1. Notions de base
2. Cibles d'attaques sur Internet
3. Tactiques de phishing
4. Infections par malwares
5. Vols de mots de passe et contrôle d'accès
6. Attaques réseau
7. Attaques du Cloud
8. Piratage du réseau sans fil
9. Casser le chiffrement
10. Analyse de risques

Calcul du risque

INFORMATION TECHNOLOGY & SOLUTIONS

- **Ex: Calculer les risques de sortir de son lit le matin**

Risk	Likelihood	Impact	Total risk
Twisted ankle	3	4	12
Step on LEGO	3	3	9
Bear attack	1	5	5

Gestion du risque

INFORMATION TECHNOLOGY & SOLUTIONS

- **Eviter le risque**
  - Ex. ne pas se lever du lit le matin, pour ne pas marcher sur une pièce le LEGO
- **Transférer le risque**
  - Ex. Si votre maison se trouve en zone inondable, payer une assurance pour couvrir les dégâts des eaux et les catastrophes naturelles
- **Atténuer le risque**
  - Ex. vérifier qu'il n'y a pas de pièces de LEGO autour de votre lit avant d'aller vous coucher ou établir une règle pour les bannir de la chambre, vous diminuez ainsi le risque de marcher sur une pièce de LEGO en vous levant le matin
- **Accepter le risque**
  - Ex. La vraisemblance d'une attaque d'ours dans votre chambre est relativement faible, il n'a aucune raison de s'en prémunir

Menaces

INFORMATION TECHNOLOGY & SOLUTIONS

- **Une menace est un impact négatif sur un système, une personne ou une organisation.**

- **Schéma de classification STRIDE (Microsoft)**
  - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges

Threat	Target
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privileges	Authorization

Mesures/Contrôles

INFORMATION TECHNOLOGY & SOLUTIONS

- **La catégorisation des menaces et des acteurs de la menace vous aide également à choisir la meilleure mesure, qui tente de prévenir ou d'atténuer une menace.**

Category	Purpose	Example
Administrative	Provides guidance on how to conduct activities	Security awareness training, policy, procedure
Preventative	Attempts to stop unwanted activity before it happens	Firewall
Detective	Attempts to discover unwanted activity after it has happened or while it's happening	IDS, logging
Compensating	Adds additional security to make up for a weakness in another control	Encryption
Corrective	Fixes another control or flaw after it's discovered	Patch management, vulnerability management

Plan de gestion de risques

INFORMATION TECHNOLOGY & SOLUTIONS

- **Pour gérer toutes les activités, vous devez utiliser un outil spécial appelé registre des risques, qui est un système permettant de documenter tous les risques que vous suivez actuellement.**

Sparkle Kitten Co. Risk Register									
Risk	Threat	Risk Impact	Risk Likelihood	Risk Score	Risk Address	Control	Control Progress	Owner	Date
Email is compromised	Phishing attempts sent by a Black Hat	4	3	12	Mitigate	Training	Implemented	Angel	5/20/2020
Kittens are not fluffy enough	Humidity makes kittens lose fluff	5	2	10	Transfer	Kitten Insurance	Not Implemented	Ted	5/20/2020
Loss of data from servers	Failure of backups system due to malware	5	3	15	Mitigate	Anti-malware software	Implemented	Cheryl	5/20/2020
Loss of data from servers	Flood in Server Room	5	1	5	Acceptable	None	NA	NA	5/20/2020

Exemple récapitulatif* 1/5

INFORMATION TECHNOLOGY & SOLUTIONS

- Imaginons que vous travailliez en tant qu'**analyste de la sécurité** pour une entreprise de taille moyenne comptant 500 employés. Une partie de votre travail quotidien consiste à **vérifier les alertes** provenant soit des employés, soit de votre **pare-feu** et de votre **système de détection d'intrusion**.

- Un matin, vous recevez un e-mail d'un employé paniqué disant qu'ils ont reçu un e-mail étrange et qu'ils ont cliqué sur le lien à l'intérieur. Maintenant, ils craignent que cela n'ait causé des problèmes sur leur ordinateur.

- **Que devez vous faire en tant qu'analyste de la sécurité?**

Exemple récapitulatif* 2/5

INFORMATION TECHNOLOGY & SOLUTIONS

- Vous vérifiez les e-mails à l'aide de certains **outils d'analyse rapide du phishing**, tels que VirusTotal et MX Toolbox.

- L'e-mail prétend être un avis de réinitialisation de mot de passe de Microsoft, mais il provient de l'adresse e-mail ***M1cos0ft.com***. En regardant le lien, vous vous rendez compte qu'il est peut-être malveillant.

- L'employé a déclaré qu'en cliquant sur le lien, il leur avait demandé de télécharger un outil de mise à jour de mot de passe qui s'exécutait ensuite sur leur ordinateur. Vous réalisez qu'il s'agit probablement d'un logiciel malveillant et **lancez une analyse antivirus** sur le système.

Exemple récapitulatif* 3/5

INFORMATION TECHNOLOGY & SOLUTIONS

- Pendant que vous analysez le système, vous **vérifiez votre pare-feu et vos alertes IDS** pour voir s'ils contiennent quelque chose de suspect. Effectivement, vous remarquez **des alertes sur le nouveau trafic potentiellement malveillant provenant de l'ordinateur de l'employé**.

- Vous ne savez pas quoi faire de ces informations, **vous transférez donc les alertes à un consultant senior en sécurité de l'équipe**. Ils regardent les alertes et réalisent que cela signifie probablement que l'employé a téléchargé **un cheval de Troie qui tente de diffuser un ransomware sur le réseau**.

- Le consultant senior en sécurité **met rapidement à jour l'IDS et le pare-feu** pour bloquer toute tentative de l'ordinateur de l'employé de se connecter à d'autres ordinateurs sur le réseau. Pendant ce temps, votre analyse récupère un kit de malware bien connu. **Vous pouvez l'isoler et supprimer l'infection**, mais **vous réinitialisez complètement l'ordinateur** de l'employé juste pour être sûr.

Exemple récapitulatif* 4/5

INFORMATION TECHNOLOGY & SOLUTIONS

- **Après l'incident**, vous et vos collègues de sécurité effectuez **une analyse post-incident** pour discuter de ce qui s'est passé et comment l'empêcher à l'avenir. Le **RSSI** anime cette réunion. De la discussion, tout le monde se rend compte que **l'organisation a un point faible: former les employés à reconnaître les emails de phishing**, qui constituent **une menace majeure**, comme en témoigne l'attaque du ransomware. **Le RSSI ajoute cela au registre des risques** de l'entreprise et discute de la meilleure façon de **mettre en œuvre le contrôle** de la formation des employés.

- Le **RSSI** présente le nouveau risque à **la réunion trimestrielle de gestion des risques** et discute de l'idée d'acheter une plate-forme de formation au phishing pour l'organisation. **Le responsable des RH est d'accord avec l'idée du RSSI**, car la plate-forme de formation actuelle utilisée par les RH n'inclut pas d'informations sur le phishing. **Le directeur financier est également d'accord** car le coût est faible mais le bénéfice serait être immense.

- Il a été décidé que le RSSI étudierait diverses options et ferait rapport au comité dans un mois avec une recommandation. **Le RSSI met à jour le registre des risques et désigne un membre de l'équipe de sécurité** pour l'aider dans cette tâche.

Exemple récapitulatif* 5/5

INFORMATION TECHNOLOGY & SOLUTIONS

- Bien qu'il s'agisse d'un scénario fictif, il représente la manière dont la sécurité doit fonctionner dans une organisation. Dans le scénario, il ne suffisait pas de gérer l'appel d'un employé à propos d'un e-mail de phishing**. L'analyste de la sécurité a dû croiser différentes sources d'informations et demander conseil aux autres membres de l'équipe pour avoir une vue d'ensemble**.

- De plus, le travail ne s'est pas arrêté une fois l'incident terminé. **Tout aussi important était le suivi, qui permis à l'organisation de reconnaître ses failles en matière de sécurité et de les corriger.** En utilisant l'expertise de l'équipe de sécurité, le RSSI a démontré avec succès pourquoi il était important de travailler avec la direction générale pour acheter la plate-forme de formation spécifique. C'est **pourquoi un plan de gestion des risques est essentiel** : il permet de lier tous les aspects de la sécurité. Cela montre le besoin de sécurité et la solution dans un format simple et facile à gérer.

Exercice*: Conduire une analyse de risque

- **Pour cet exercice final, choisissez une cible et effectuez une analyse de risque par rapport à celle-ci. Une analyse des risques définit tous les risques pour une cible et examine le processus de gestion des risques pour chacun d'entre eux. Votre cible peut être votre domicile, votre université, votre entreprise ou tout autre endroit où vous avez une bonne idée des menaces ou des risques de cybersécurité qui existent. Une fois que vous avez choisi votre cible, complétez les étapes suivantes :**

1. Identifiez tous les actifs que vous souhaitez inclure dans votre analyse.
2. Enregistrez toutes les façons dont vous pensez que ces actifs pourraient être attaqués ou endommagés. Lorsque vous faites cela, n'oubliez pas d'effectuer le test de cohérence en considérant la probabilité d'une attaque.
3. Examinez toutes les manières dont vos actifs peuvent être attaqués et regroupez-les à l'aide du modèle STRIDE. Identifiez ce que les attaques ont en commun. Ce sont les menaces qui pèsent sur votre cible.
4. Déterminez lequel de vos regroupements a le plus grand nombre d'instances. Plus le nombre d'instances est élevé, plus la probabilité est élevée. Ajoutez également une note rapide sur l'impact potentiel.
5. Placez les menaces dans un registre des risques, comme celui illustré plus haut dans ce chapitre. Incluez le risque, la menace et le score de risque.
6. Regardez quels contrôles vous avez mis en place pour faire face à ces attaques.
7. Remplissez le registre des risques avec la façon dont vous gérez le risque et les contrôles que vous utilisez pour faire face au risque.

Takeaways

INFORMATION TECHNOLOGY & SOLUTIONS

- **Réfléchissez à deux fois avant de cliquer. Même les pros se font avoir quand ils sont trop pressés!**
- **Prenez le temps de mettre en place les mesures appropriées. Les travaux de cybersécurité semblent parfois fastidieux mais ne peuvent pas être remis au lendemain.**
- **Ne croyez jamais quelqu'un sur parole, vérifiez par vous-même. Si vous n'êtes pas sûr qu'une configuration soit bien faite, ne supposez pas que quelqu'un d'autre va s'en occuper!**
- **Demandez toujours de l'aide. La cybersécurité n'est pas une « île » et ne se limite pas à son équipe.**
- **Continuez à lire et à apprendre. La cybersécurité nécessite de se former constamment pour garder une longueur d'avance sur les pirates.**
- **S'amuser et prendre plaisir! La cybersécurité est une affaire sérieuse, mais cela ne veut pas dire qu'elle doit rester grave et stricte.**

Et surtout retenez l'équation :

INFORMATION TECHNOLOGY & SOLUTIONS

Connaissance + Expérience + Prudence

=

Confiance et Sécurité

L'IA et la Cybersécurité

INFORMATION TECHNOLOGY & SOLUTIONS

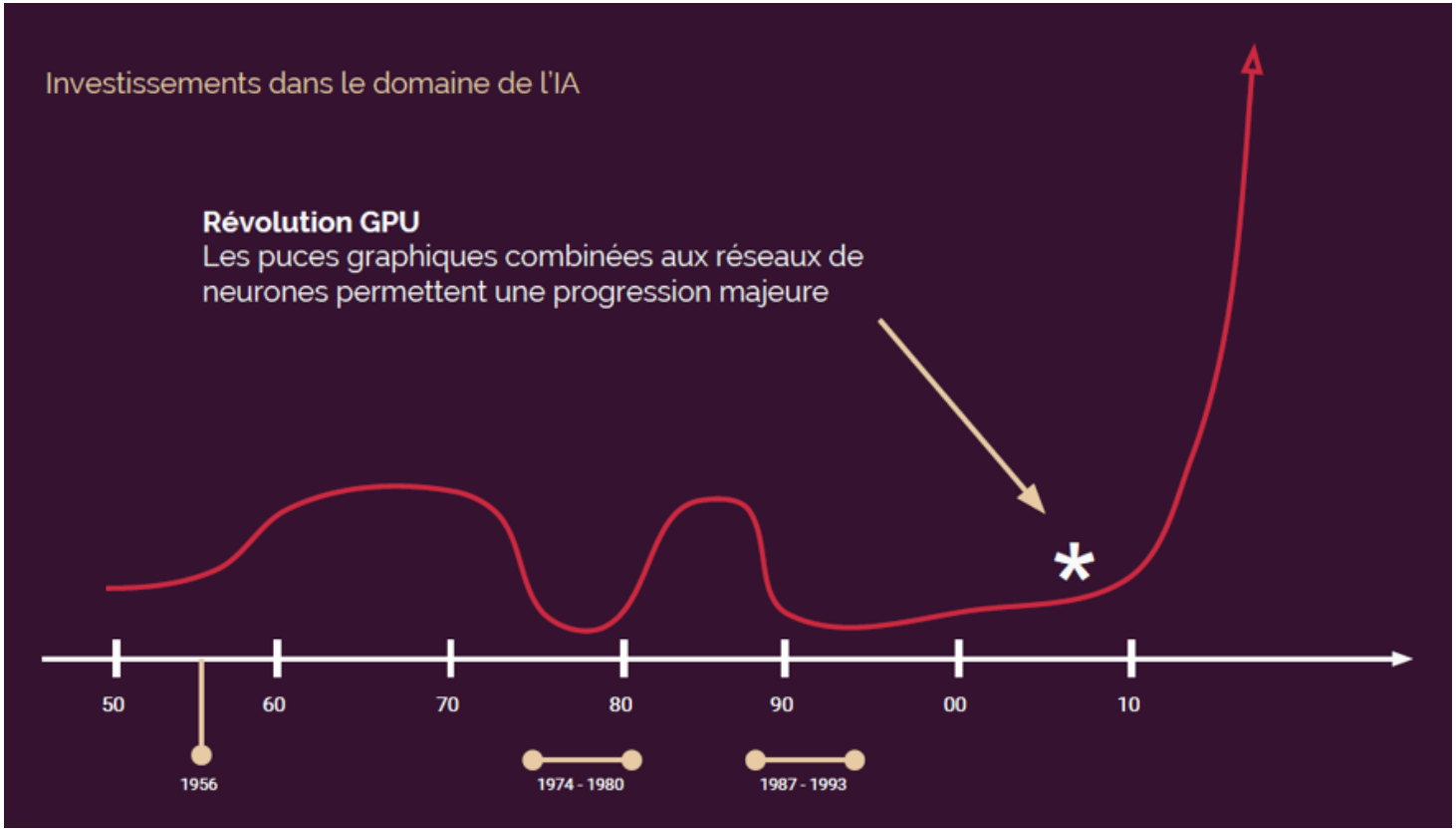
- La cybersécurité est une industrie technique qui se développe très rapidement. Cela est en partie dû à l'augmentation des objets connectés mais surtout à cause de la prolifération des cybermenaces.

- Selon une étude récente de la société de cybersécurité Sophos, les attaques de ransomware sont plus fréquentes : 66 % des entreprises interrogées ont été touchées par des ransomwares en 2021, contre 37 % en 2020. Le nombre de rançons payées est plus élevé : en 2021, 11 % des entreprises ont déclaré avoir payé des rançons de 1 million de dollars ou plus (environ 860 000 €), contre 4 % en 2020.

- Dans ce contexte, nous avons besoin d'une technologie qui peut renforcer l'industrie de la cybersécurité, une technologie disruptive qui peut nous aider à protéger nos données et même nos vies humaines.

- L'Intelligence Artificielle (AI) fait partie de ces révolutions technologiques qui peuvent changer fondamentalement le domaine de la cybersécurité.

L’IA et la Cybersécurité



L'IA et la Cybersécurité

INFORMATION TECHNOLOGY & SOLUTIONS

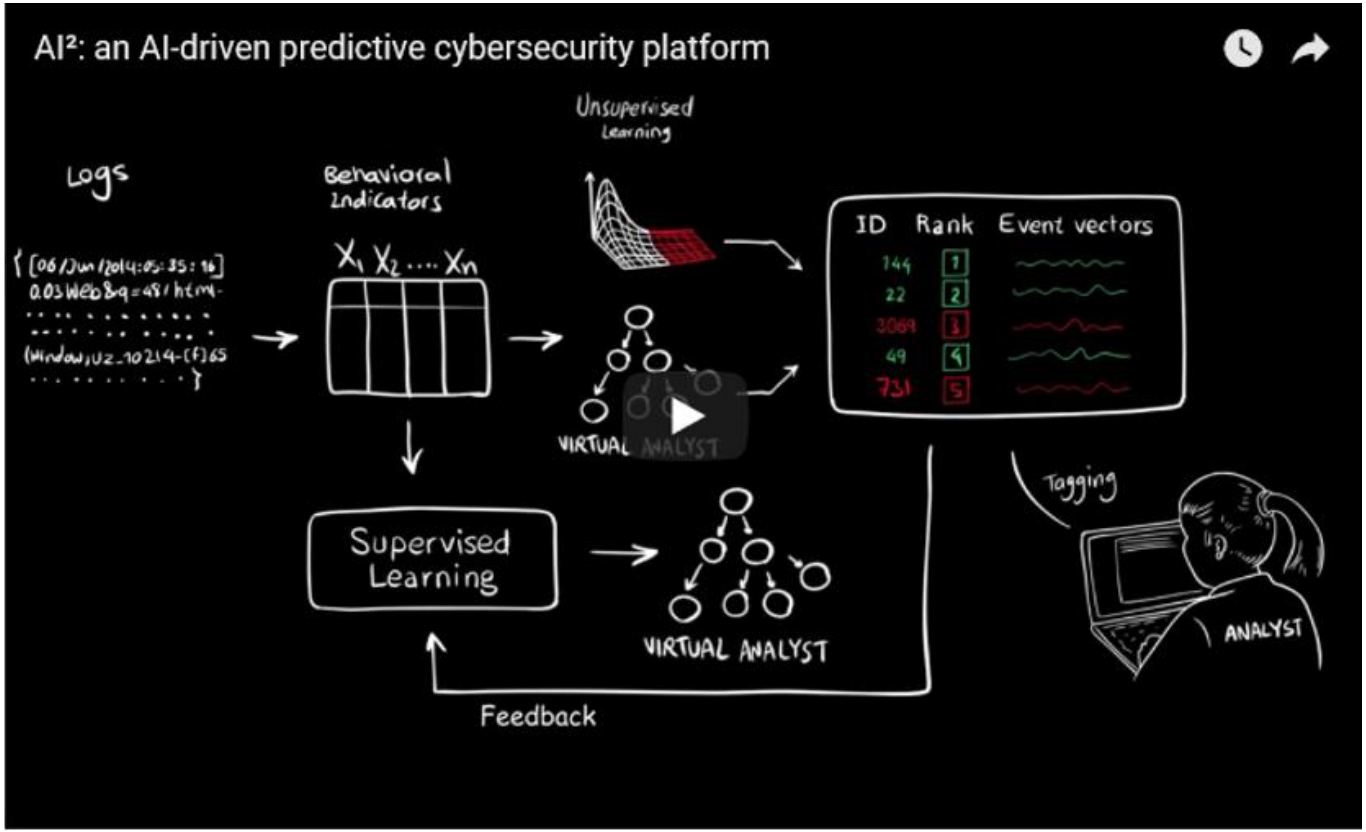
- L'IA fait référence à une intelligence quasi-humaine ou surhumaine conférée à un être artificiel, c'est-à-dire, une machine. Cette technologie couvre un ensemble de spécialités qui incluent, entre autres, l'informatique, la linguistique, la physique et les mathématiques.

- L'IA a été développée pour permettre aux machines de penser et d'agir comme de vrais humains. Elle permet aux machines de résoudre des problèmes qu'une équipe d'experts humains mettrait des années à surmonter.

- Aujourd'hui, les entreprises ont beaucoup de mal à identifier une vulnérabilité sécurité. Elles ont besoin pour cela de nombreux experts en cybersécurité. Même lorsqu'elles les possèdent, il reste difficile de trouver une anomalie dans un système et d'anticiper une menace latente ou furtive (type APT – Advanced Persistent Threat).

- C'est là que l'IA a un rôle important à jouer en étant capable d'analyser des quantités importantes de données pour trouver très rapidement les anomalies et les menaces. .

L’IA et la Cybersécurité



L’IA et la Cybersécurité

INFORMATION TECHNOLOGY & SOLUTIONS

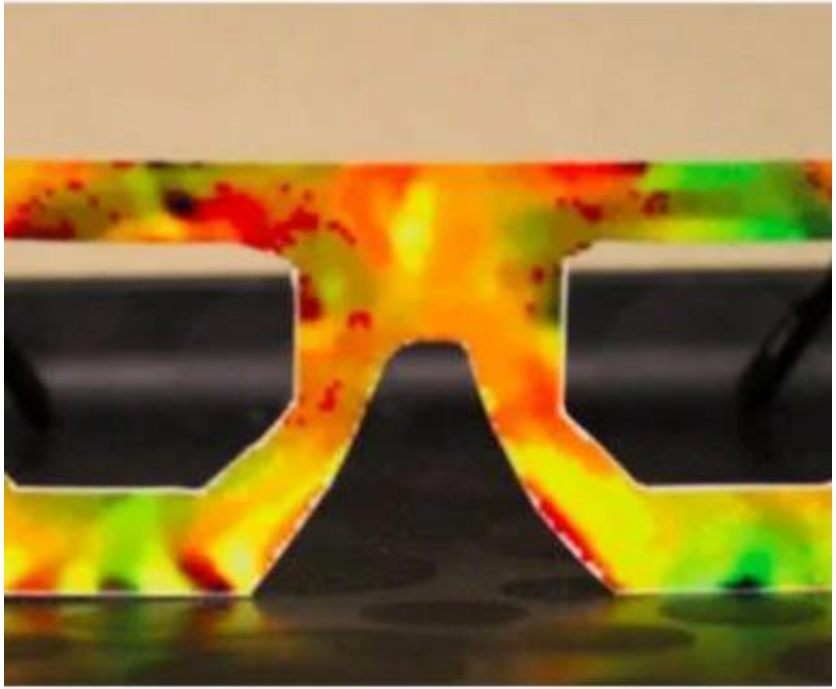
- L’IA est-elle un danger pour l’expert humain? L’IA a encore besoin d’un opérateur humain pour l’interaction et l’apprentissage. On estime qu’avec l’association de l’IA avec l’humain, plus de 85% des cyberattaques pourront être empêchées.

- L’IA est-elle une menace pour la cybersécurité? L’IA est une arme à double tranchant. Si elle peut aider les experts sécurité à trouver des anomalies, elle peut être aussi utilisée par les hackers pour développer des attaques plus précises et plus efficaces.

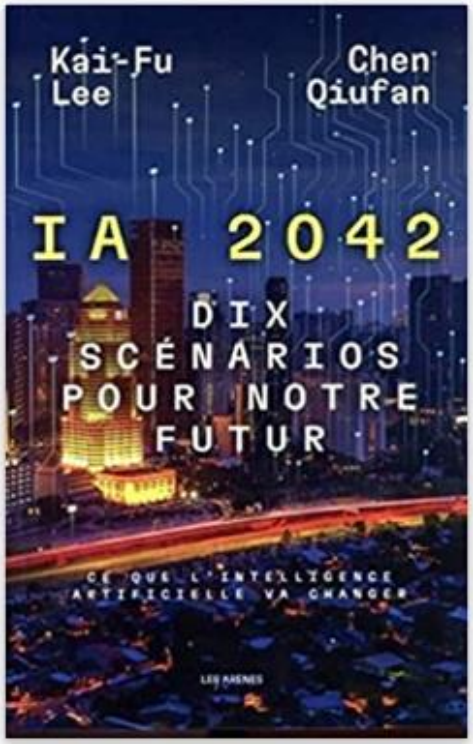
- Le futur de l'IA et de la cybersécurité est difficile à prédire mais il y a un potentiel énorme à combiner les 2 technologies. Utilisées à bon escient, elles peuvent aider les entreprises à réduire, voire à contrer les prochaines cyberattaques.

L’IA et la Cybersécurité

INFORMATION TECHNOLOGY & SOLUTIONS



Le futur de l'IA!



I.A 2042 - Dix scénarios pour notre futur Broché – Livre grand format, 20 octobre 2022

de Chen Qiufan (Auteur), Kai Fu-Lee (Auteur), & 2 plus

#1 Meilleure vente dans Intelligence artificielle

Afficher tous les formats et éditions

Broché
24,90 € prime

1 D'occasion à partir de 22,00 €
3 Neuf à partir de 24,90 €

Livraison GRATUITE (0,01€ pour les livres) **en point retrait (selon éligibilité des articles).** Détails

Questions/Réponses

INFORMATION TECHNOLOGY & SOLUTIONS

Pour conclure

INFORMATION TECHNOLOGY & SOLUTIONS

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

"si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous ne comprenez pas les problèmes et vous ne comprenez pas la technologie."

“When a big company lays you off, they often give you a year's salary to 'go pursue a dream.' If you're stupid, you panic and get another job. If you're smart, you take the money and use the time to figure out what you want to do next.”

«Quand une grande société vous licencie, ils vous donnent souvent un an de salaire pour «aller poursuivre votre rêve.» Si vous êtes stupide, vous paniquez et trouvez un autre emploi. Si vous êtes intelligent, vous prenez l'argent et utiliser ce temps pour déterminer ce que vous voulez faire après."

Bruce Schneier
Cybersecurity Expert

MASTER SYSTÈMES D'INFORMATION, RÉSEAUX ET NUMÉRIQUE

Dauphine UNIVERSITÉ PARIS | PSL