



Cybersécurité



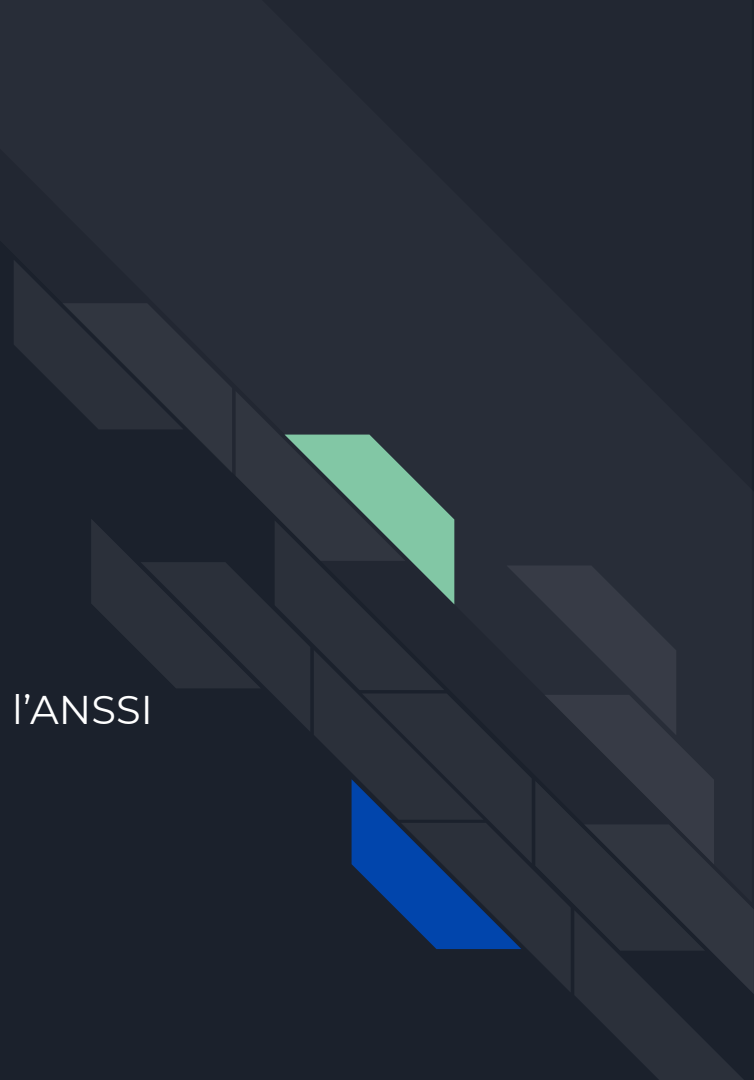
Whoami

- Olivier LASNE
- Pentester depuis 5 ans
- Indépendant
- Passionné depuis longtemps par Linux et le logiciel libre.



“Plus notre société se numérise, plus elle s'expose aux risques inhérents à ces technologies.”

Manifeste de l'ANSSI





Objectifs

Présenter :

- le contexte et les enjeux
- le vocabulaire
- les référentiels et ressources



Contexte et enjeux

Source : ANSSI

“ À périmètre équivalent sur ces attaques traitées par l’ANSSI (impact fort en sécurité nationale ou économique), [...]

on était à 54 attaques en 2019 et on est 128 au 30 septembre de cette année. “

Guillaume Poupard,
Directeur Général de l’ANSSI





Interventions de l'ANSSI en 2019

 2 296 Signalements

 370 Incidents

 9 Incidents Majeurs

 16 opérations de cyberdéfense

Exemple de Cyberattaque

PIXELS • SÉCURITÉ INFORMATIQUE

Partage



Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs

Le centre hospitalier, qui compte près de 2 500 lits d'accueil, se remet progressivement de la paralysie informatique provoquée par un virus de type rançongiciel.

Par Gilles Triolier • Publié le 18 novembre 2019 à 22h59 - Mis à jour le 19 novembre 2019 à 05h45

🕒 Lecture 4 min.

Une hausse de la Cybercriminalité

- 9 Français sur 10 ont été confrontés à un acte de malveillance sur Internet *
- 90 000 victimes assistées par cybermalveillance.gouv.fr (augmentation de 210%)

Les grandes tendances :

- Hameçonnage (phishing)
- Arnaque au faux support technique
- rançongiciels
- chantage à la webcam prétendue piratée





Histoire



Quelques dates

Années 70 et 80 :

- Cap'n Crunch (Phone Phreaks) dans les années 70
- Début des activités de Kevin Mitnick (arrêté en 95)
- 1981 : création du Chaos Computer Club (Allemagne)
- 1985 : Création du webzine Phrack

Années 90 et 2000 :

- 1993 : 1ère DEF CON
- 1999 : 1er Chaos Communication Camp
- 2000 : le ver ILOVEYOU infecte le monde entier (milliards de dollars de perte)
- 2003 : création de Anonymous



Quelques dates

Années 2000 et 2010 :

- 2005 : ver XSS Samy infecte MySpace
- 2006 : création de Wikileaks
- 2010 : Stuxnet
- 2011 : Piratage du Playstation Network
- 2013 : PRSIM révélé par Edward Snowden
- 2013 : Silk road fermé par le FBI
- 2017 : ransomware WannaCry et Petra



Quelques groupes de hacker connus

- NSA : National Security Agency, agence de renseignement américaine
- APT1 (Unité 61398) : section de l'armée Chinoise, en charge des opérations militaires dans les réseau informatique
- Syrian Electronic Army
- Shadow Broker

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with diagonal stripes.

Les phases d'une attaque



Les phases d'une attaque

1. Reconnaissance

- Identifier les cibles potentielles
- Recherche d'information publique
- Scan de vulnérabilités

2. Intrusion et Présence

- Exploitation d'une vulnérabilité
- Phishing



Les phases d'une attaque

3. Mouvement Latéral

- Infecter d'avantage de systèmes
- Cartographie du réseau interne

4. Acquisition des privilèges administrateurs

- Compromission de serveurs interne
- Identifiants mal protégés

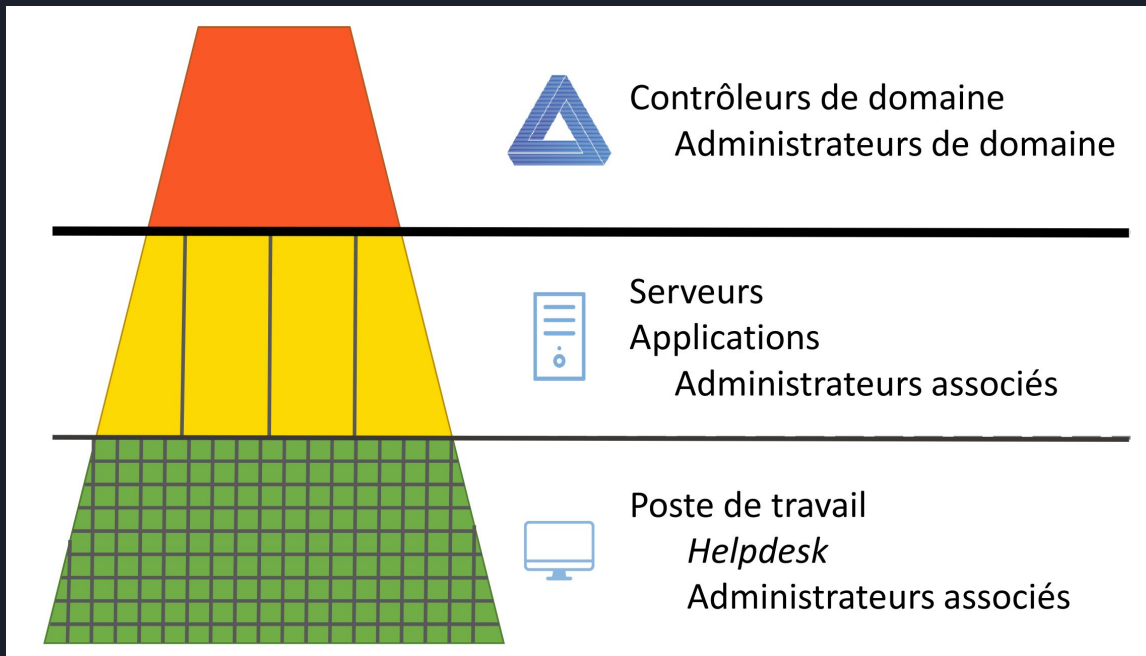


Les phases d'une attaque

5. Mission achevée

- Nettoyage des traces
- Maintient d'accès
- Exfiltration de données

Pyramide d'administration



Source STTIC 2017: administration en silo

Quelques définitions





Définition

La **Sécurité des Systèmes d'Information (SSI)** est l'ensemble des moyens :

- Techniques
- Organisationnels
- Humains
- Juridiques

visant à empêcher l'utilisation non autorisée du Système d'Information.



Objectifs de sécurité - CID

- Confidentialité : seul les personnes autorisées ont accès
- Intégrité : les données n'ont pas été modifiées
- Disponibilité : il est possible d'accéder aux données



Types de hacker

- Black Hat : hacker malveillant, recherche généralement le profit
- White Hat : hacker éthique / professionnel s'assure de la sécurité des systèmes d'informations
- Grey Hat : bienveillant mais n'a pas l'autorisation de tester un système d'information

APT - Advanced Persistent Threat

- Groupe de hacker discret, qui cherche à maintenir un accès
- Le plus souvent un état (ou soutenu par un état)
- Une liste est maintenue par le MITRE





Blue & Red Team

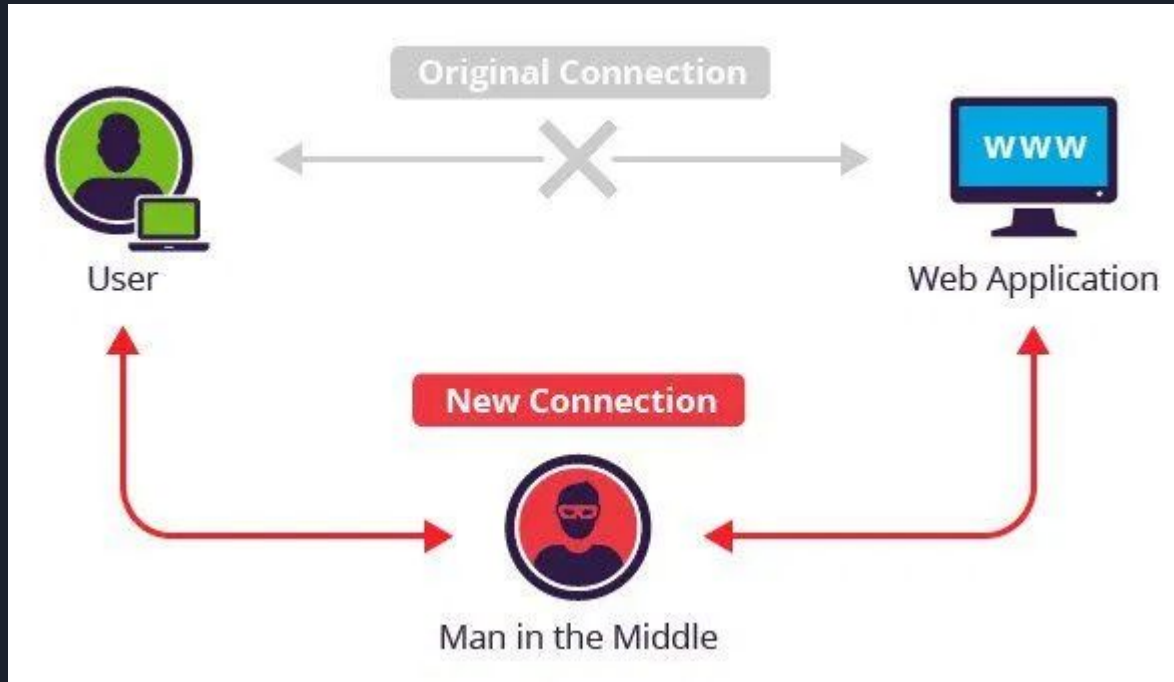
- Blue Team : équipe en charge de sécuriser les réseaux
- Red Team : équipe en charge de tester la sécurité (tests offensifs)
- Purple Team : attaque et défense, ou partage d'information entre les équipes




Exploit & co

- Vulnérabilité : faille de sécurité dans un programme
- Exploit : programme ou script qui exploite une vulnérabilité
- Shell : accès interactif en ligne de commande
- Reverse Shell : shell depuis la machine victime qui vient se connecter sur notre machine
- RCE : remote code execution = exécution de code à distance
- Malware : logiciel malveillant

Man-In-The-Middle (MITM)





Différents types d'attaques



Exploitation d'une vulnérabilité

- Un attaquant identifie une vulnérabilité sur une machine
- Il l'exploite attaque ainsi le système d'information
- Cas classique des sites internet qui ont beaucoup de données utilisateur
- Simulé par les tests d'intrusion externe



Ingénierie Sociale

- Un attaquant identifie des employés et mène une campagne de Phishing
- Une pièce-jointe malveillante est envoyée et permet d'obtenir un accès initial dans le réseau de l'entreprise visée
- Méthode encore très efficace aujourd'hui
- Variante : usurpation d'identité et manipulation de la cible (ex : support informatique)
- Testé généralement lors des tests d'intrusion Red Team



Autres méthodes

- Shoulder surfing : regarder par dessus l'épaule de l'administrateur
- Eavesdropping : écouter les conversations
- Dumpster Driving : fouiller les poubelles.



Attaques physiques

- S'introduire dans l'entreprise, et accéder aux serveurs
- Keylogger physique : enregistre les frappes de clavier d'un ordinateur (attaque de la femme de ménage)
- Lock Picking : crochétage de serrures
- Obtenir un accès au réseau interne (ex : LAN Turtle)



Métiers de la cybersécurité



Métiers de la Cybersécurité

- **Gestion de la sécurité et pilotage des projets de sécurité**
 - Directeur Cybersécurité
 - Responsable de la Sécurité des Systèmes d'Information (RSSI)
 - Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE
 - Coordinateur sécurité
 - Directeur de programme de sécurité
 - Responsable de projet de sécurité
- **Conception et maintien d'un SI sécurisé**
 - Chef sécurité de projet
 - Architecte sécurité
 - Spécialiste sécurité d'un domaine technique
 - Spécialiste en développement sécurisé
 - Cryptologue
 - Administrateur de solutions de sécurité
 - Auditeur de sécurité organisationnelle
 - Auditeur de sécurité technique



Métiers de la Cybersécurité

- **Gestion des incidents et des crises de sécurité**
 - Responsable du SOC
 - Opérateur analyste SOC
 - Responsable du CSIRT
 - Analyste réponse aux incidents de sécurité
 - Gestionnaire de crise de cybersécurité
 - Analyste de la menace cybersécurité
- **Conseil, services et recherche**
 - Consultant en cybersécurité
 - Formateur en cybersécurité
 - Évaluateur de la sécurité des technologies de l'information
 - Développeur de solutions de sécurité
 - Intégrateur de solutions de sécurité
 - Chercheur en sécurité des systèmes d'information



Lois

Le fait **d'accéder** ou de se maintenir, frauduleusement, dans tout ou partie d'un **système de traitement automatisé de données** est puni de deux ans d'emprisonnement et de **60 000 € d'amende**.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **trois ans d'emprisonnement et de 100 000 € d'amende**.

Article 323-2

Peut monter jusqu'à 10 ans d'emprisonnement et 300 000€ d'amende

Le fait d'**introduire frauduleusement des données** dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement** et de **150 000 € d'amende**.

Article 323-3

Le fait, sans motif légitime, notamment de sécurité informatique, de détenir, ou de **mettre à disposition** un **programme informatique conçu** pour commettre une ou plusieurs des **infractions** [...] est puni des peines prévues respectivement pour l'infraction elle-même.

Article 323-3-1
(édité)



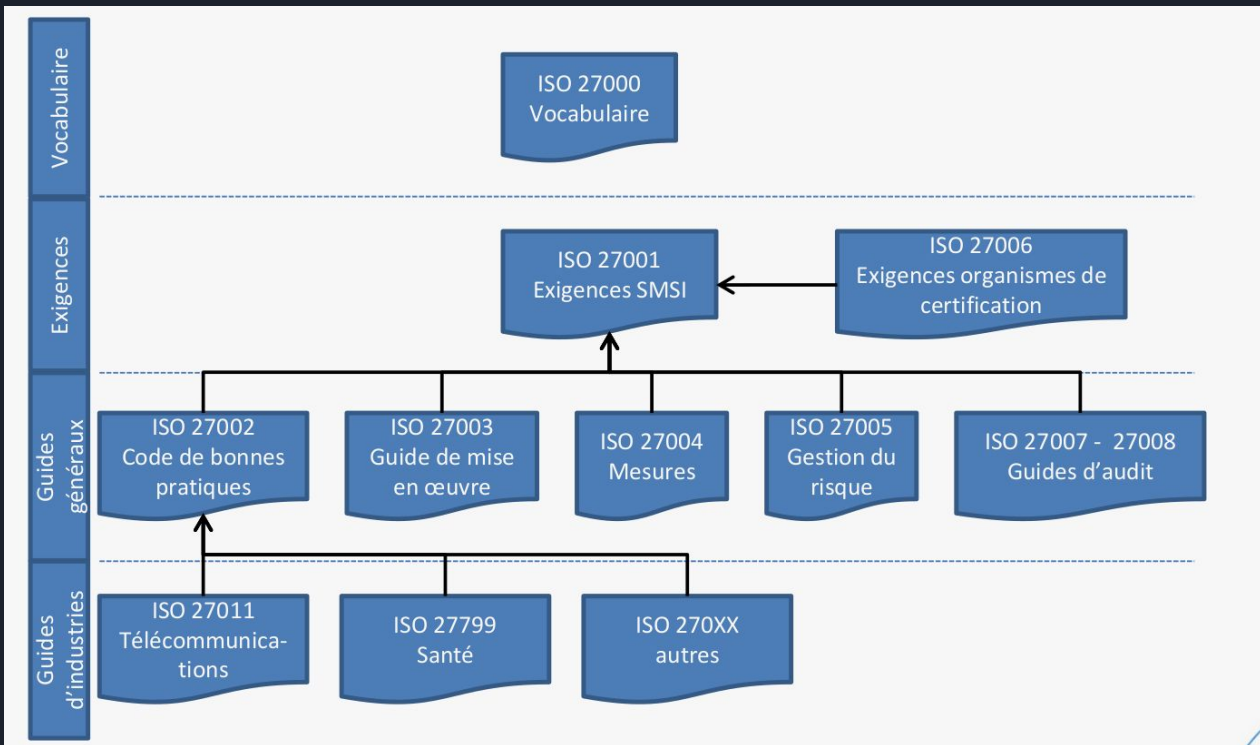
Législation sur les données

- Loi informatique et Liberté : encadre les données personnelles
 - RGPD (Règlement général sur la protection des données) : texte européen sur la protection de données personnelles
-
- PASSI (LPM) : Produits et Prestataires de services qualifiés par l'ANSSI
 - RGS (référentiel général de sécurité) : Guide de sécurisation édité par l'ANSSI

Normes et référentiel



ISO 27000





PTES

- Penetration Testing Execution Standard
- Guide / Méthodologie sur la manière de réaliser un test d'intrusion
- [http://www.pentest-standard.org/index.php/PTES Technical Guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines)



OWASP

- Open Web Application Security Project
- Top 10 OWSAP : top 10 des vulnérabilités web
- méthodologie de test
- support de formation



CVE, CVSS

- CVE : identifiant d'une vulnérabilité (facilite la recherche et la coopération)
- CVSS : Score de criticité d'une vulnérabilité

Les CVE sont maintenues par le MITRE.

La NVD (national vulnerability database) donne un score CVSS. Elle est maintenue par le NIST.

ATT&CK : Liste de méthodes d'attaque maintenue par le MITRE

Exemple de CVE

CVE-2020-16119 Detail

Current Description

Use-after-free vulnerability in the Linux kernel exploitable by a local attacker due to reuse of a DCCP socket with an attached dccps_hc_tx_ccid object as a listener after being released. Fixed in Ubuntu Linux kernel 5.4.0-51.56, 5.3.0-68.63, 4.15.0-121.123, 4.4.0-193.224, 3.13.0-182.191 and 3.2.0-149.196.

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



CNA: Canonical Ltd.

Base Score: 6.3 MEDIUM

Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.



Ressources



Ressources

Sécurité Web :

- Web Application Hacker handbook : très (trop) complet
- <https://portswigger.net/web-security>

CTF / pentest :

- Hackthebox, vidéos de ippsec
- root-me.org

Exploitation de binaires:

- liveoverflow sur youtube
- site de CTF



FIN