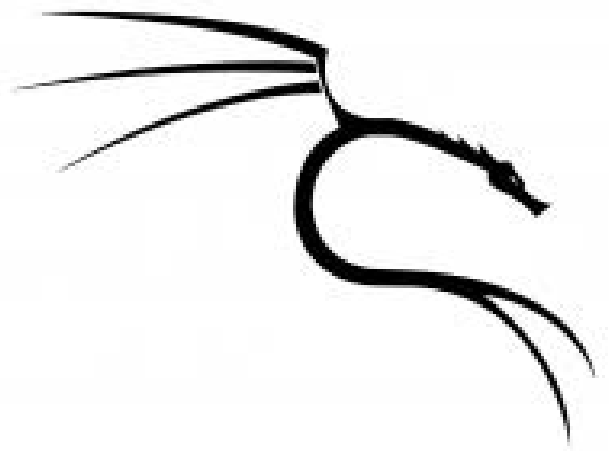
# Sécurité Informatique

Eric BERTHOMIER

eric.berthomier@free.fr

31 mars 2019



# Qui je suis ?

- Master en Informatique Système (Bac +4)

# Qui je suis ?

- Master en Informatique Système (Bac +4)
- Développeur Système (SSII)

# Qui je suis ?

- Master en Informatique Système (Bac +4)
- Développeur Système (SSII)
- Administration Système Réseau Sécurité (SSII)

# Qui je suis ?

- Master en Informatique Système (Bac +4)
- Développeur Système (SSII)
- Administration Système Réseau Sécurité (SSII)
- Sécurité Informatique - Spécialisation Forensic (Ministère)

# Qui je suis ?

- Master en Informatique Système (Bac +4)
- Développeur Système (SSII)
- Administration Système Réseau Sécurité (SSII)
- Sécurité Informatique - Spécialisation Forensic (Ministère)
- Sécurité Informatique - CSSI (Ministère)

# On se voit ...

2 demi-journées pour éviter un mauvais clic.

# 1ère demi-journée

- Introduction

# 1ère demi-journée

- Introduction
- Discussion ouverte

# 1ère demi-journée

- Introduction
- Discussion ouverte
- Pause

# 1ère demi-journée

- Introduction
- Discussion ouverte
- Pause
- Principes généraux de la sécurité informatique

# 1ère demi-journée

- Introduction
- Discussion ouverte
- Pause
- Principes généraux de la sécurité informatique
- Grands principes de fonctionnement d'un système d'exploitation et des applications

# 1ère demi-journée

- Introduction
- Discussion ouverte
- Pause
- Principes généraux de la sécurité informatique
- Grands principes de fonctionnement d'un système d'exploitation et des applications
- Présentation de SysInternals - ProcessExplorer

# 1ère demi-journée

- Introduction
- Discussion ouverte
- Pause
- Principes généraux de la sécurité informatique
- Grands principes de fonctionnement d'un système d'exploitation et des applications
- Présentation de SysInternals - ProcessExplorer
- Présentation des sujets SSI

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté
  - Cas pratique : Des manœuvres simples pour éviter le risque

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté
  - Cas pratique : Des manœuvres simples pour éviter le risque
- Travaux Pratiques : utilisation de SysInternals

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté
  - Cas pratique : Des manœuvres simples pour éviter le risque
- Travaux Pratiques : utilisation de SysInternals
  - Process Explorer

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté
  - Cas pratique : Des manœuvres simples pour éviter le risque
- Travaux Pratiques : utilisation de SysInternals
  - Process Explorer
  - TcpView

# 2nde demi-journée

- Présentation par les étudiants des travaux de recherche
- Discussion ouverte
- Pause
- Cas pratique : Le PDF
  - Structure d'un PDF
  - Cas pratique : Exfiltration de données au travers d'un PDF
  - Cas pratique : PDF infecté
  - Cas pratique : Des manœuvres simples pour éviter le risque
- Travaux Pratiques : utilisation de SysInternals
  - Process Explorer
  - TcpView
  - AutoRuns

# On commence - Discussion ouverte

## Jeu de rôle

Deux scénarios,

- *"On vous donne 2.000 BitCoins pour ralentir gentiment le concurrent de votre entreprise"*
- *"Virez pour un motif non acceptable, vous décidez de vous venger de votre entreprise. Vous disposez pour cela de 2.000 BitCoins*

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques
- Stockage / Élaboration d'un mot de passe : entre risques et praticité

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques
- Stockage / Élaboration d'un mot de passe : entre risques et praticité
- SSL : une sécurité ou un risque mesuré

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques
- Stockage / Élaboration d'un mot de passe : entre risques et praticité
- SSL : une sécurité ou un risque mesuré
- Zero Day

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques
- Stockage / Élaboration d'un mot de passe : entre risques et praticité
- SSL : une sécurité ou un risque mesuré
- Zero Day
- Le Dark Net : principe et réalité

# Sujets proposés ou à proposer ...

- Contre-mesure par rapport à l'anti-spam
- Smartphone et Ordinateur : Le meilleur ou le pire
- Ingénierie sociale
- VBA (Excel / Word), risques
- Télémaintenance : avantages et risques (DragonFly)
- Le prix d'une donnée
- Base de données : concepts et risques
- Stockage / Élaboration d'un mot de passe : entre risques et praticité
- SSL : une sécurité ou un risque mesuré
- Zero Day
- Le Dark Net : principe et réalité
- Sécurité du code