cetic
Your Connection to ICT Research

Cybersécurité Industrielle

Sécurité des installations

M. Bouhou

www.enmieux.be
Cofinancé par l'Union européenne
Wallonie
official partner | digital wallonia .be

Centre d'Excellence en **Technologies** de l'**Information** et de la **Communication**
www.cetic.be

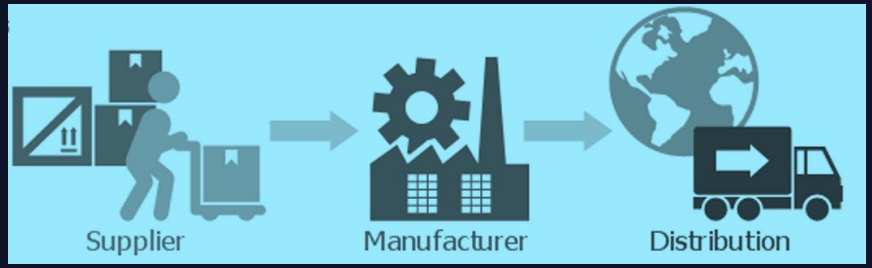
Qui suis-je ?

- **Malik Bouhou**
- **3 ans de recherche en Cybersécurité @CETIC**
- **12 ans dans le secteur public : IT project, Security Advisor, Dev, Admin Sys, …**
- **J'adore comprendre comment fonctionnent les « choses » / things**
- **J'adore trouver comment utiliser ces « choses » à ma façon**
- **Passionné par les cyberattaques intelligentes… mais pas par leurs conséquences néfastes**
- **Je voudrais faire de toutes ces « choses » connectés un endroit plus sûr**
- **Rendre la sécurité accessible à tous**

WalHub: Focus sur les entreprises manufacturières

cetic
Your Connection to ICT Research

Environ **500 services** WalHub toucheront **>200 PME** d'ici fin 2025



4 « digital enablers »

- Internet des objets (iot)
- Intelligence artificielle (ia)
- Calcul haute performance (hpc)
- Cybersécurité

Les services de WalHub sont accessibles **gratuitement** (aide *de minimis*) depuis l'information et la démonstration en collectif (workshops, visites…) jusqu'à l'accompagnement individuel

WALHUB
BOOST YOUR DIGITAL TRANSFORMATION

sirris AGORIA the strength of a trusted community
PÔLE MECATECH LE PÔLE DE COMPÉTITIVITÉ WALLON EN GÉNIE MÉCANIQUE
LOGISTICS WALLONIA connect move share
Multitel INNOVATION CENTRE
Cenaero
IDELUX en partenariat avec l'ESA via HESTIA

Avec le support de :
Agence du Numérique

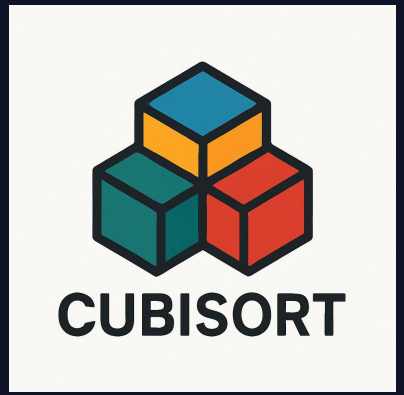
Agenda

- **Cas d'utilisation**
- **Tests de pénétration sur les systèmes industriels**
  - Inputs
  - Information gathering
  - Reconnaissance
  - Vulnerability Assessment
  - Deep Dive and Exploitation
  - Reporting and Recommendations

Cas d'utilisation

Découvrez Cubisort

- Chez Cubisort, nous sommes spécialisés dans le tri de précision des cubes pour les applications industrielles, scientifiques et créatives. Pour garantir que vos cubes contiennent suffisamment d'anneaux métalliques, nous utilisons nos systèmes de tri de pointe pour assurer une classification impeccable à grande échelle. Des chaînes de production aux kits pédagogiques, nous organisons vos cubes de manière efficace, fiable et innovante.
- Nous avons cette splendide machine de triage que vous pouvez voir ici.



En tant que client potentiel, je me demande

- Mon cube est-il en sécurité chez Cubisort ?
- Pensez-vous qu'il soit sécurisé contre les cyberattaques ?
- Pouvez-vous le prouver ?

Tests de pénétration

Définition du NIST : « Méthode de test dans laquelle les testeurs ciblent des composants binaires individuels ou l'application dans son ensemble afin de déterminer si des vulnérabilités intra- ou inter-composants peuvent être exploitées pour compromettre l'application, ses données ou ses ressources environnementales.

Wikipedia : « Un test d'intrusion, communément appelé pentest, est une cyberattaque simulée autorisée sur un système informatique, réalisée pour évaluer la sécurité du système ;[1] il ne faut pas le confondre avec une évaluation de vulnérabilité.[2] Le test est réalisé pour identifier les faiblesses (ou vulnérabilités), y compris le potentiel pour des parties non autorisées d'accéder aux fonctionnalités et aux données du système,[3][4] ainsi que les forces,[5] permettant de réaliser une évaluation complète des risques.

⇒ Les définitions sont axées sur l'IT, car l'activité provient de l'IT.

⇒ Now, we know you can't only consider cybersecurity in the IT

⇒ Les objectifs sont axés sur l'IT, mais équivalents pour d'autres systèmes ou produits.

⇒ Évaluez la sécurité de votre produit/système

⇒ Confirmez vos risques/analyse des risques

⇒ Évaluez la réponse de votre produit/système lors de cyberattaques simulées.

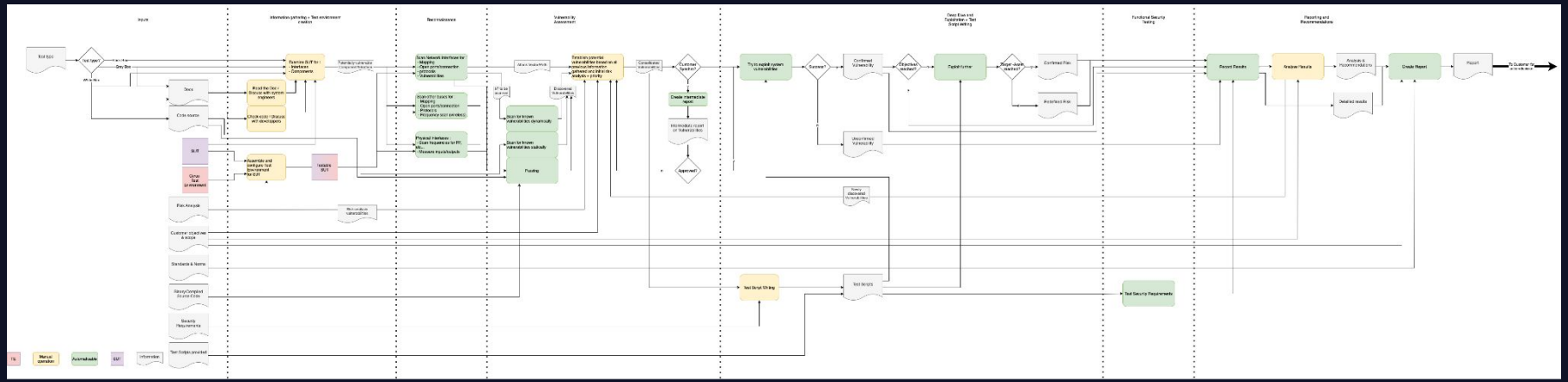
Tests de pénétration

Cette activité repose généralement sur l'expertise des testeurs d'intrusion et les phases sont souvent similaires dans les différentes normes et standards, mais le reste relève uniquement de la méthode de travail / l'approche de l'expert.

Nous souhaitions définir un processus plus reproductible, permettant d'identifier les activités à automatiser.

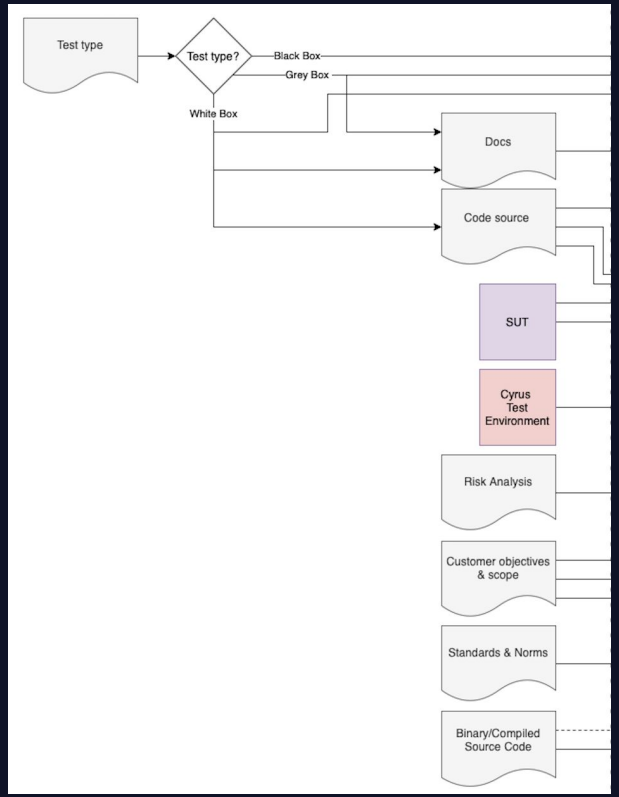
Le processus :

Inputs ⟶ Information Gathering ⟶ Reconnaissance ⟶ Vulnerability Assessment ⟶ Script Writing ⟶ Reporting and recommendations



Phases des tests de pénétration

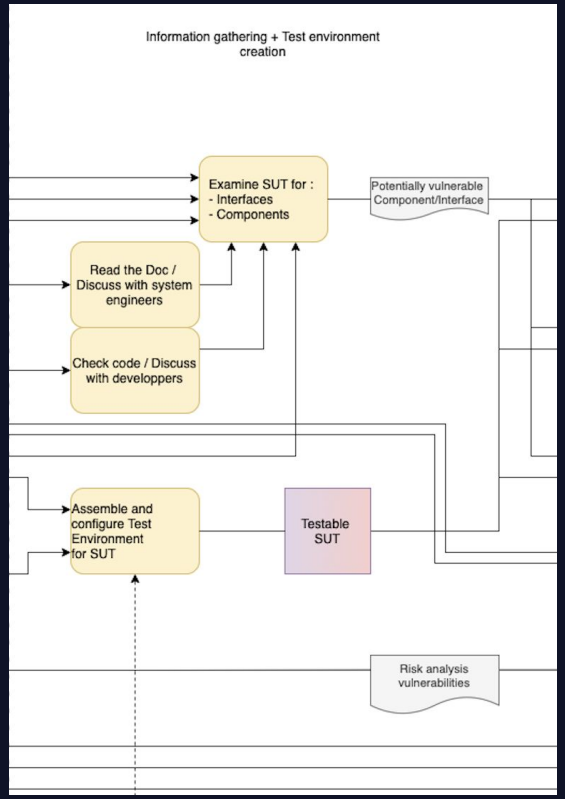
- Inputs (Entrées)



- Le SUT = System Under Test = Système soumis aux tests
- Le ROE = Rules of engagement = Règles d'engagement
  - Objectifs et périmètre du fournisseur du SUT
- Informations sur le SUT => détermine le type de test :
  - Boîte noire
  - Boîte grise
    - Documentation
  - Boîte blanche
    - Documentation
    - Code source
    - Configuration
    - Accès
- Analyse de risques
- …

Phases des tests de pénétration

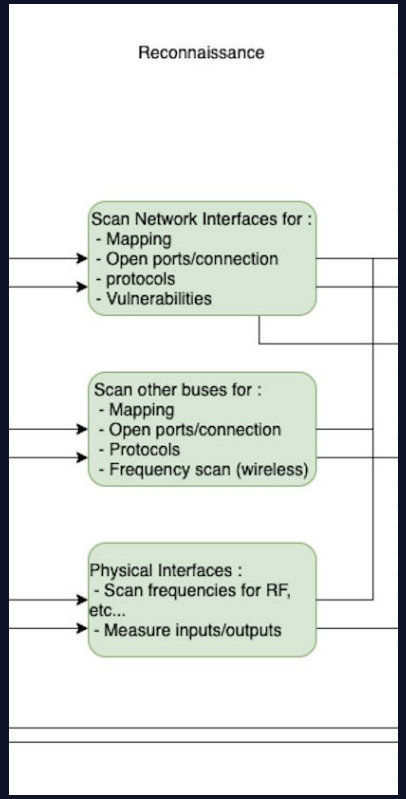
- Information gathering (Collecte d'informations)



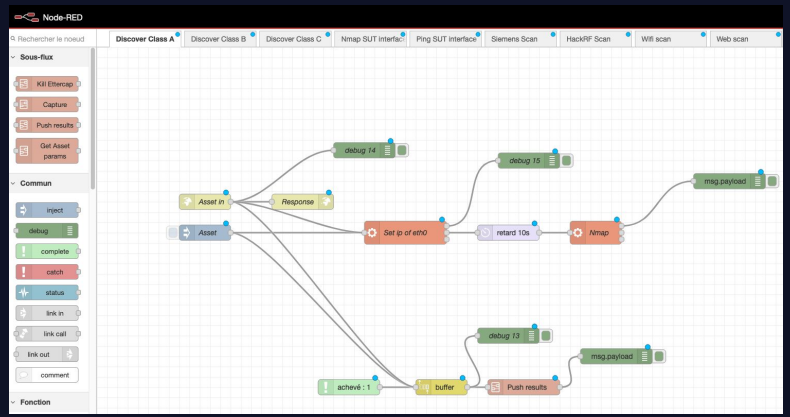
- Présentation / Démonstration du SUT
- Opérations manuelles
- Inspection visuelle
- Extraction d'informations à partir des données d'entrée
- Recherche sur Internet
- C'est également à ce moment-là que nous assemblons notre environnement de test et le SUT.
- Aucune interaction pour l'instant.

Penetration Testing Phases

- Reconnaissance

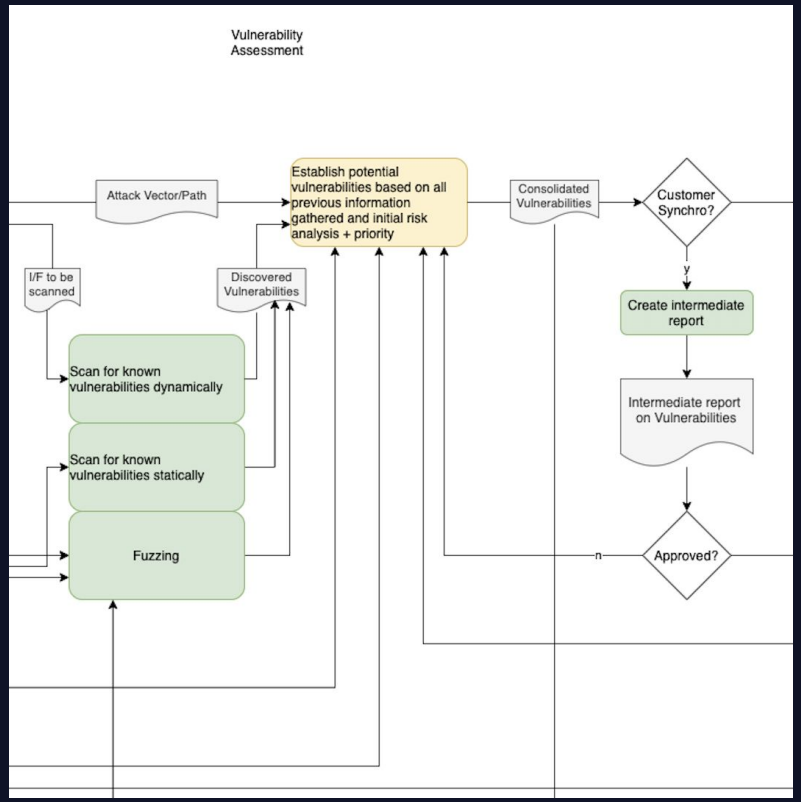


- Reconnaissance = non intrusive
- La partie la plus courante consiste en la reconnaissance du réseau
- Dans nos cas, d'autres interfaces sont fréquemment utilisées :
  - Physiques (capteurs/actionneurs)
  - RF
  - Bus industriels (Modbus, OPC UA, etc.)
  - …
- Automatisation via une plateforme low-code (Node-RED)



Penetration Testing Phases

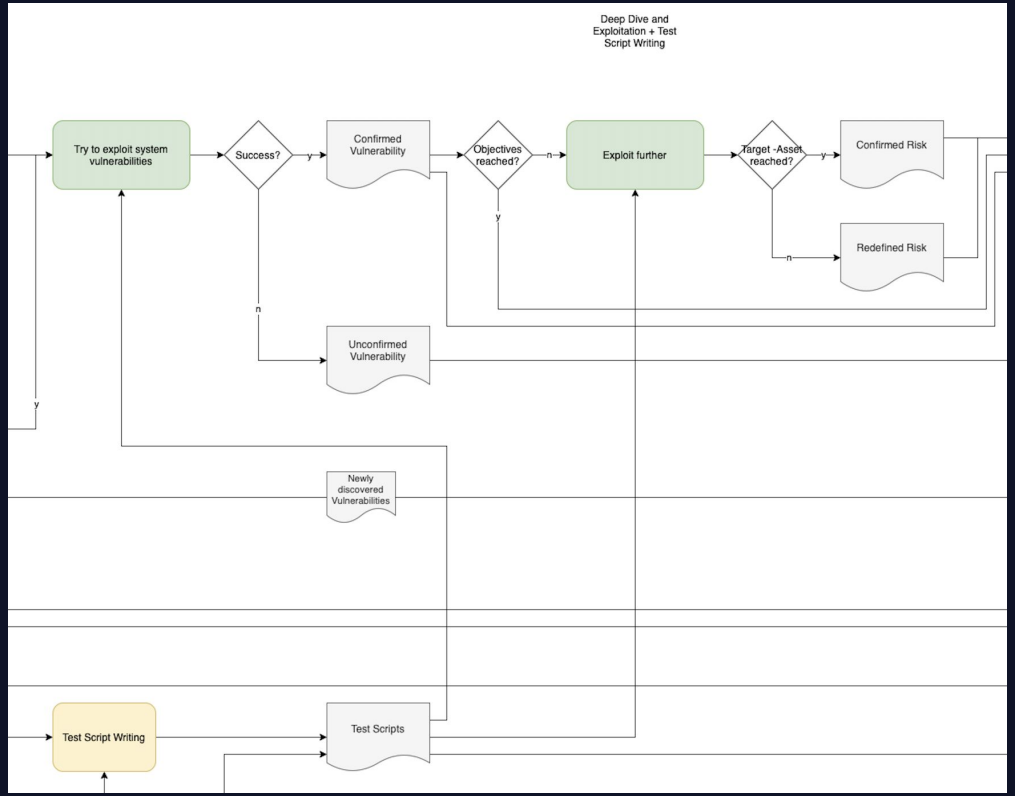
- Vulnerability Assessment (Évaluation de la vulnérabilité)



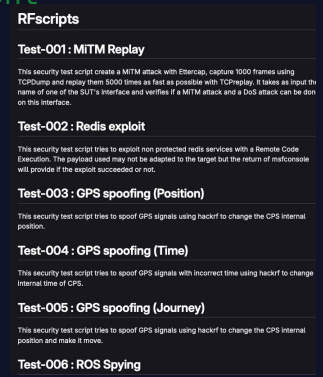
- Manuel :
  - cve.mitre.org
  - cvedetails.com
  - github.com
  - duckduckgo.com
  - LLMs?
  - …
- Automatique :
  - Les scanners de vulnérabilités tels que Greenbone Vulnerability Manager, ZAP, …
  - Principalement au niveau des interfaces réseau
  - Code source -> SonarQube, Dependency Check, …
- Cela peut être un bon moment pour une discussion intermédiaire avec les partenaires
  - Aucune intrusion n'a encore eu lieu.
  - La suite est plus claire.

Penetration Testing Phases

- Deep Dive and Exploitation (Exploration en profondeur)

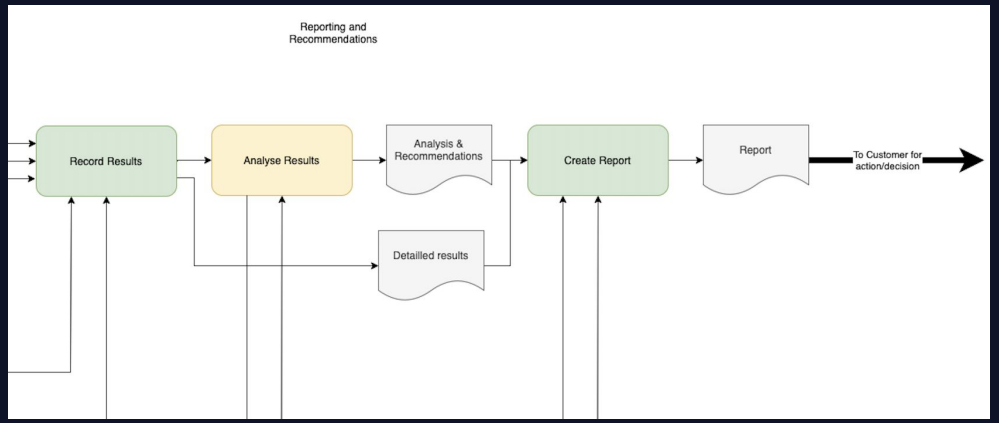


- Voici la partie amusante !
- De nombreuses ressources sont disponibles.
  - exploit-db.com
  - metasploit
  - github.com
  - LLMs?
  - Your skills
- Test manuel
- Test automatisé avec une plateforme de test



Penetration Testing Phases

- Reporting and Recommendations (Rapports et recommandations)



- Il est temps d'informer les partenaires du SUT de vos découvertes.
- Mais surtout, comment y remédier !

https://docs.google.com/document/d/1nXVH5qF-QbRCqbEFP4MQRV4iGDKaIJ4IpomOin41N2E/edit?usp=sharing

Any Questions?

cetic
Your Connection to ICT Research

Workshop - Cyrus/Walhub

Malik Bouhou

Ingénieur de recherche Sénior

+32 471 46 53 17

malik.bouhou@cetic.be

cetic

Your Connection to ICT Research

Avenue Jean Mermoz 28
6041 Charleroi - Belgique

IBAN : BE66 7320 3594 7443
BE 0474.549.932
RPM : Charleroi

twitter.com/@CETIC
twitter.com/@CETIC_be

linkedin.com/company/cetic

info@cetic.be

+32 486 182477

www.cetic.be