KNOCKKNOCK

Outsmart the threat!

L'IA au service des red team

UNE ENTREPRISE ACCOMPAGNÉE PAR UNITEC

RÉGION Nouvelle-Aquitaine

bpifrance

La Banquiz
Open source start-up program

08 | 03 | 2022

PLAN

CHAÎNE DE VALEUR DES RED TEAMS

CHAÎNE DE VALEUR DES RED TEAMS

Se mettre à la place de potentielles menaces

Identifier les **vulnérabilités**

Éprouver les équipes et les systèmes de défense

Corriger les failles et bloquer les chemins d'attaque avant que des attaquants ne les exploitent

Confronter les chemins d'attaque découverts

Aux **incidents de sécurité vécus** et enregistrés

Aux **événements redoutés** identifiés lors des analyses de risque

Aux **tracés d'attaque** dessinés au "stabilo" sur un diagramme du SI

KNOCKKNOCK

LIMITATIONS ET POTENTIEL D'AMÉLIORATION

BY DESIGN

Un défenseur doit protéger **toute sa cage** de but
alors qu'un attaquant n'a besoin que d'**une seule brèche pour marquer**.
La dissymétrie est inhérente au jeu.

LIMITATIONS ET POTENTIEL D'AMÉLIORATION

COÛT & DURÉE

*"**Dans le temps imparti aux tests d'intrusion**,*
nous avons pu identifier les vulnérabilités suivantes
ou encore nous avons réussi à prendre le contrôle de telle ou telle ressource du système d'information ..."

LIMITATIONS ET POTENTIEL D'AMÉLIORATION

RÉPLICABILITÉ

Le pentest c'est comme un **sportif de haut niveau**. Sans formation ou **entraînement**, sans partages et **challenges**, les muscles s'atrophient, les habitudes se perdent, et on se retrouve dépassé en un rien de temps.

LIMITATIONS ET POTENTIEL D'AMÉLIORATION

POINT D'ANCRAGE

Connectivité de **départ** qui **conditionne** à fortiori
la **visibilité** dont dispose le pentester vis-à-vis de la cible.
Ancrage **externe** ou **interne** ?

LIMITATIONS ET POTENTIEL D'AMÉLIORATION

TYPOLOGIE D'ATTAQUANT

Quel **typologie** de **menace** évaluons-nous ?

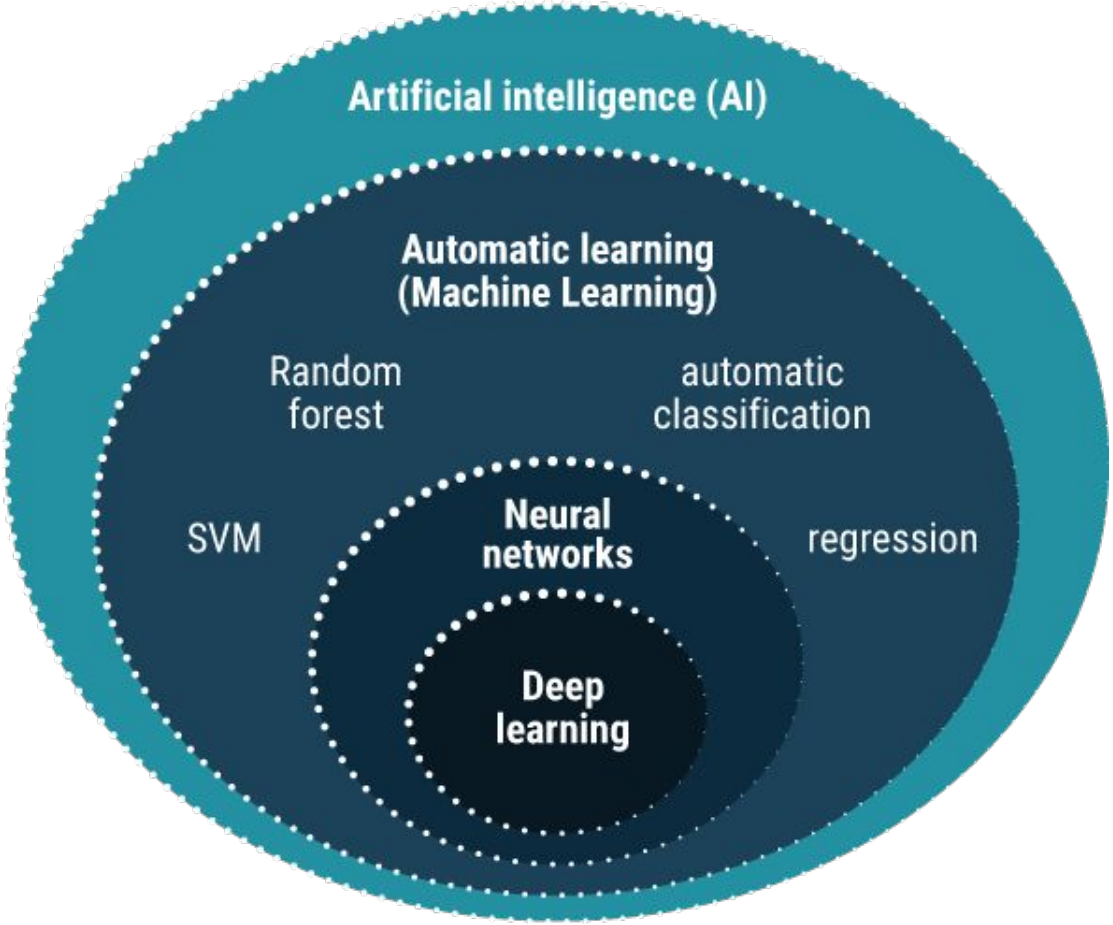
L'IA AU SERVICE DES RED TEAMS

QUELLES IA POUR QUELLES SOLUTIONS

1. Qu'est-ce que l'IA ?
2. L'IA dans la boîte à outils du Hacker Éthique
3. L'IA en autonomie
4. Les bénéfices de l'IA
5. Les limites et les risques futurs

QUE CACHE LE MOT “IA” ?

QUE CACHE LE MOT “IA” ?



KNOCKKNOCK

QUE CACHE LE MOT “IA” ?

SYSTÈMES EXPERTS

Scripté
Ensemble de règles écrites par des experts humains

LIMITES

On ne connaît pas forcément les règles de résolution d’une problématique donnée
Les règles que nous connaissons ne sont pas forcément optimales
Ces systèmes sont complexes et potentiellement difficiles à maintenir dans le temps
...

MACHINE LEARNING

Approches probabilistes
(réseaux bayésiens par exemple)
Arbres de décisions
(Random forest, gradient-boosted trees ...)
Réseaux neuronaux artificiels
(Deep learning, Réseaux de convolutions, Technologies d’attention ...)
...

OBJECTIF

Apprendre les règles de résolutions d’une problématique donnée

L'IA DANS LA BOÎTE À OUTILS DU HACKER ÉTHIQUE

IDENTIFICATION DES CIBLES

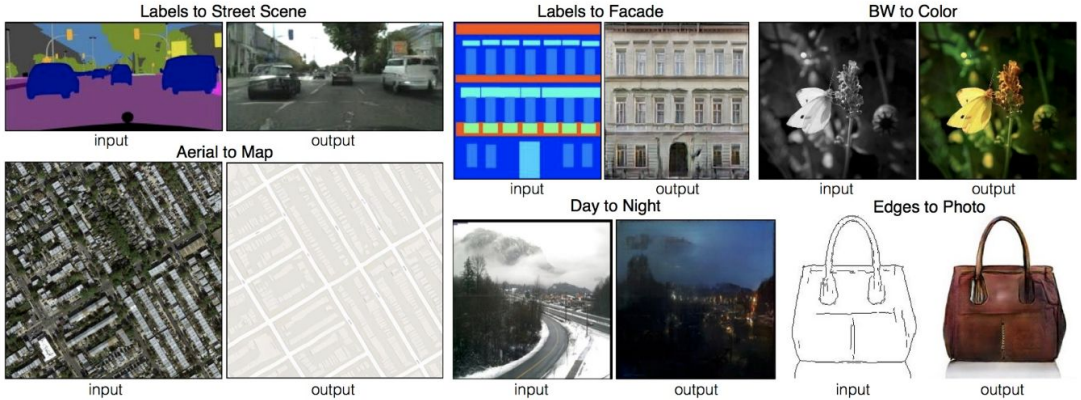
TECHNOLOGIE
Classification

INTÉRÊT
Identification des **services**, **technologies**, **versions**...
A partir des **headers**, **formats de retour**, **code source de pages web**, **captures d'écran**, ...

RESSOURCES INTÉRESSANTES
Projet open source
https://github.com/gyoisamurai/GyoiThon
(approche statistique Naive Bayes pour identifier des technos à partir de mots clés)

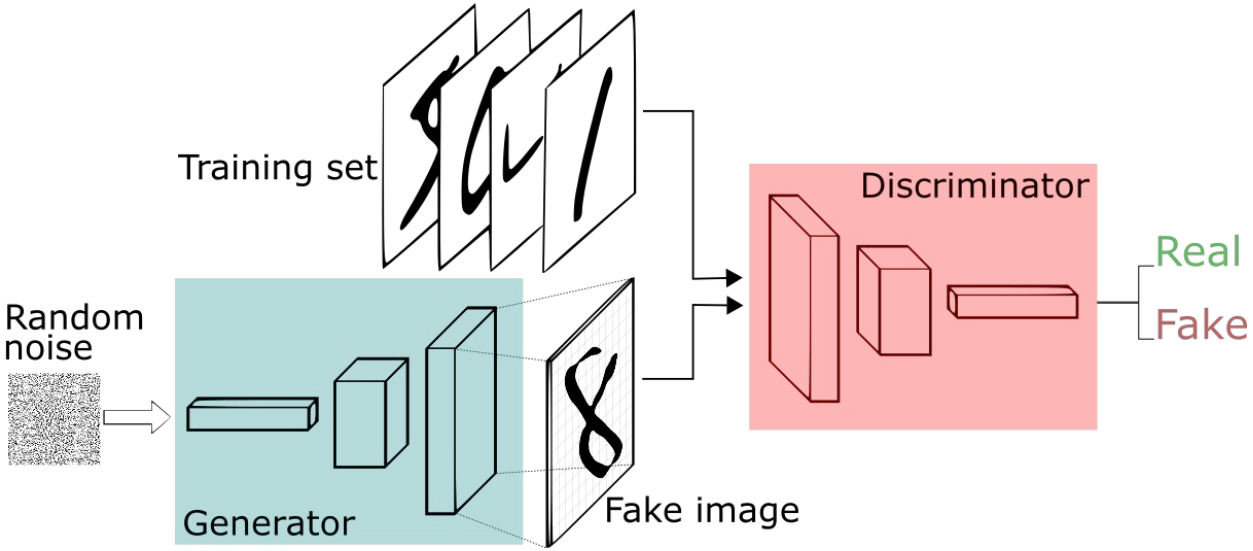
Modèles générateurs & Deepfakes

GÉNÉRATION ET CAMOUFLAGE DE CODES MALVEILLANTS : LES GANS



KNOCKKNOCK

GÉNÉRATION ET CAMOUFLAGE DE CODES MALVEILLANTS : LES GANS



Modèles générateurs & Deepfakes

GÉNÉRATION ET CAMOUFLAGE DE CODES MALVEILLANTS

TECHNOLOGIE

GAN, technologie générative de code

Entraîner à la fois un générateur (attaque) et un détecteur (défense)

INTÉRÊT

Bypasser les systèmes de détection de codes malveillant

Générer à la volée le **code d'injection adéquat** en fonction du contexte de l'attaque

RESSOURCES INTÉRESSANTES

Projets open source

https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/Generator (approche adversariale et génétique de la génération de code d'injection pour détecter une XSS et bypasser des WAF)

https://deepmind.com/blog/article/Competitive-programming-with-AlphaCode (génération de code automatique pour répondre à des challenges de code)

Modèles générateurs & Deepfakes

SOCIAL ENGINEERING

TECHNOLOGIE

GAN, technologie générative de code

génération de son, génération de texte, génération d'images, génération de visages

Classification

INTÉRÊT

Simulation de phishing augmenté :

Génération automatique de "faux" mails / photos / voix etc ...
Identification automatique des employés plus "faibles" à partir de toutes leurs infos publiques (réseaux sociaux etc ...)

RESSOURCES INTÉRESSANTES

Projets open source

https://gizmodo.com/bank-robbers-in-the-middle-east-reportedly-cloned-someo-1847863805

Vol de 35M$ en utilisant un deepfake de voix (Janvier 2021)

https://www.silicon.fr/avis-expert/phishing-des-campagnes-a-grande-echelle-automatisee-par-lintelligence-artificielle

https://openai.com/blog/better-language-models

L'IA POUR L'AUTONOMIE

L'IA POUR AUTONOMIE

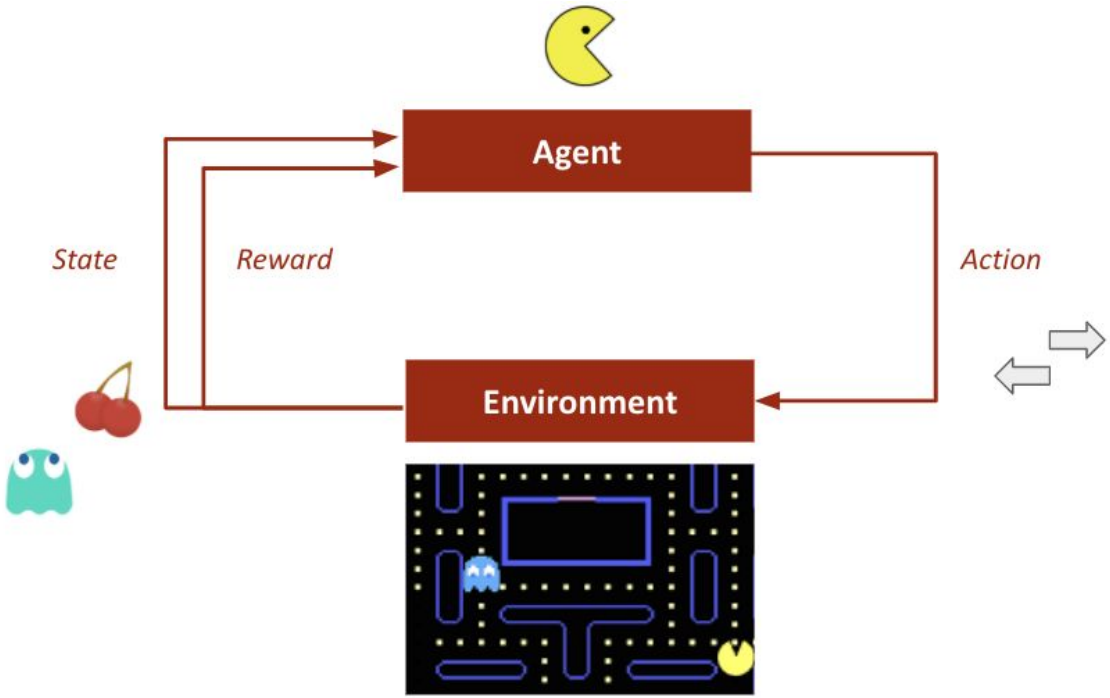
FOCUS TECHNO - Apprentissage par renforcement

AlphaGo (DeepMind) - Go
2016

OpenAI Five - DOTA
2019

L'IA pour autonomie

FOCUS TECHNO APPRENTISSAGE PAR RENFORCEMENT



KNOCKKNOCK

Internaliser les compétences d'audit

COUVERTURE PERMANENTE

Un pentester autonome permettrait :

- Internalisation des compétences d'audit
- Couverture permanente des chemins d'attaque
- Pilotage des risques cyber par la qualité et non pas la quantité

Comportements autonomes & Apprentissage par renforcement

EXPLORATION ET ENTRAÎNEMENT SUR DES TYPOLOGIES D'ATTAQUES DIFFÉRENTES ET SPÉCIFIQUES

TECHNOLOGIE

Apprentissage par renforcement

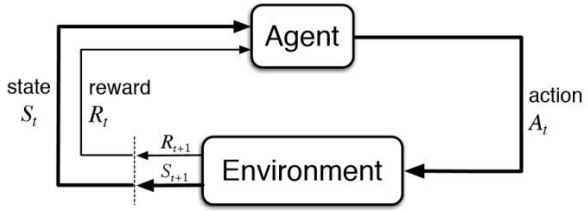
Mise en place d'un comportement autonome

INTÉRÊT

Mettre en place des **typologies d'attaques différentes** et spécifiques

Se concentrer sur les profils d'attaques apportant le plus de **valeur à l'entreprise**

Avoir des attaques plus **variées et "inattendues"** que par du "breach and attack simulator"



RESSOURCES INTÉRESSANTES

Projets open source

https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit

Apprentissage par renforcement pour sélectionner des exploits metasploit à partir des résultats d'un nmap

https://github.com/microsoft/CyberBattleSim

Simulateur pour entrainer des IA attaquants et des IA défenseurs

Apprentissage ‘online’

APPRENDRE LES FAIBLESSES DE SES CIBLES ET SE “SPÉCIALISER” FACE À UN SI “DURCI”

- Possibilité de faire évoluer son comportement au fur et à mesure du temps
- Utilisation des inputs du RSSI pour explorer de nouveaux chemins d’attaque
- Spécialisation sur le SI de l’utilisateur pour exploiter ses faiblesses

LES BÉNÉFICES DE L'IA

Les bénéfices de l'IA

L'IA RÉPOND AUX ENJEUX DES AUDITS CYBER

- Automatique donc Illimité
- Configurable et Flexible
- Traçable
- Reproductible
- ...

KNOCKKNOCK

LES LIMITES (actuelles) DE L'IA

LES LIMITES ACTUELLES AINSI QUE LES RISQUES FUTURS

- La techno semble être **suffisamment mature** et la recherche commence à vraiment aborder la question
- Données d'apprentissage
- Enjeux de Qualification et de contrôle de cette IA, **risque pour l'intégrité du SI**
- Risque d'**usages néfastes ou détourné**
- Ne pas être un énième **outil non actionnable** pour les utilisateurs
- Attention à l'effet **buzzword** "IA", il faut avant tout se concentrer sur la valeur apportée dans la sécurisation des entreprises !
- La mise en place de ces technologies demande des **ressources** et des **compétences** non négligeables

ET KNOCK KNOCK DANS TOUT ÇA ?

KNOCKKNOCK

NOUS RENFORÇONS LES CAPACITÉS DES RESPONSABLES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Nous permettons des **évaluations plus fréquentes**
sur des **périmètres plus importants**
pour **dépasser le niveau des attaquants**

Vision

NOTRE HACKER IN RESIDENCE SIMULE AUTOMATIQUEMENT DES ATTAQUES CYBER

Cartographie du système d'information

Découverte des failles et chemins d'attaque

Analyse et priorisation

- AUTOMATIQUE
- EXHAUSTIF
- CONTRÔLÉ

KNOCKKNOCK

Équipe

DES ASSOCIÉS COMPLÉMENTAIRES : TECHNOLOGIE + PRODUIT + BUSINESS

Hadi El-Khoury

DIRECTEUR PRODUIT

Expertises clés

Expert cybersécurité et test d'intrusion
Entrepreneuriat

Rôle

Expertise cyberdéfense
Go to market produit

Léo Dupouy

CTO

Expertises clés

Responsable d'équipe technique
Intelligence Artificielle

Rôle

R&D IA
Développement produit

Arthur Duchet-Suchaux

CEO

Expertises clés

Design produit
Organisation agile
Marketing de l'innovation

Rôle

Stratégie marketing & vision
Organisation

KNOCKKNOCK

Merci de votre attention

Suivez nous sur linkedin ! knock-knock-fr

Contactez-nous :

contact@knock-knock.fr

KNOCK KNOCK

MERCI

KNOCKKNOCK