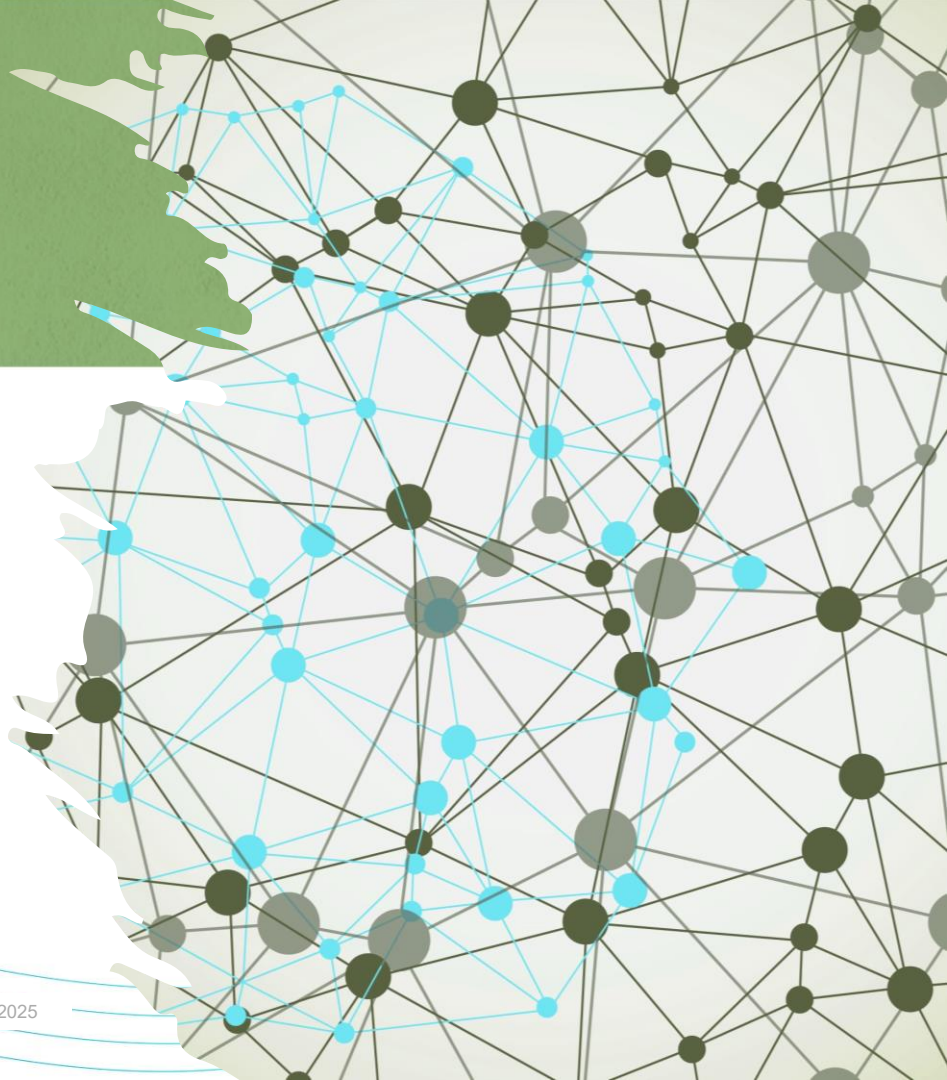
CYBERESIST

Le pont entre scanneurs de vulnérabilités et pentesteurs



© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

11/09/2025

Background

- Formateur et pentesteur
- Certifications : OSCP, CHFI, AWAE (Pentest, Forensic, Osint)
- Créateur plate-forme Cyberesist

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Constats

Les audits sont chers et complexes

Ils demandent beaucoup d'expertises alors que la réglementation les rend obligatoires (DORA, NIS2)

L'augmentation des risques

Avec les services Cloud, les accès distants, etc.

Augmentation du nombre d'attaques

Ransomwares, phishing, attaques web, attaques social-engineering

Nécessité de répéter les audits régulièrement

Un audit ne vaut pas que pour un moment donné (J).

Périmètre à auditer en extension

Cloud, web, interne, applications mobiles, etc.

Besoin d'audits pour plein de besoins

Conformité, nouvelles mises en prod, etc.

Si grands périmètres

Audits très chers onéreux

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Bref besoin d’auditer !

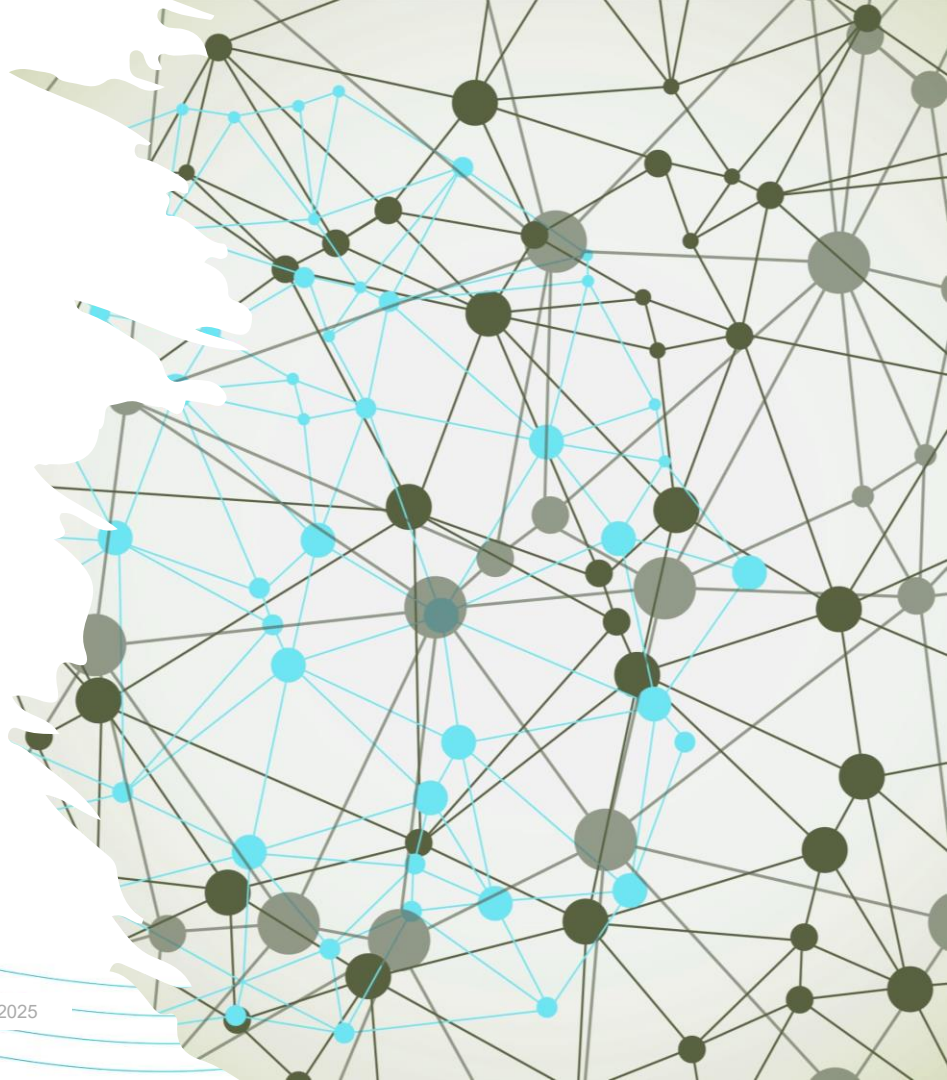
RSSIs -> s’auditer
MSSPs -> auditer ses clients
Blue team -> détecter ses vulnérabilités / s’améliorer

2 choix :

- Audits automatisés (via des scanneurs de vulnérabilités)
- Tests d’intrusion

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Forces et faiblesses des scanneurs et des pentesteurs



© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Scanneurs de vulnérabilités : Forces

Patch-management

Détectent rapidement logiciels obsolètes / non à jour

Couts maitrisés

Solutions open source ou commerciales accessibles, scans réguliers

Rapidité

Efficaces pour les vulnérabilités "simples" (services exposés, versions vulnérables).

Automatisable & industrialisable

Possible de programmer des scans réguliers (hebdo/mensuel) sans intervention humaine.

Faible barrière d’entrée

Utilisable par des profils non experts (administrateurs systèmes/réseaux).

Hygiène de base

Détecte 80% des problèmes “basiques” qui représentent déjà une grosse part du risque réel.

Conformité et audits

Répond facilement aux exigences réglementaires (ISO 27001, PCI-DSS, NIS2, etc.)

Scanneurs de vulnérabilités : Faiblesses

Surfaces limitées

Ne scannent que ce qu'ils voient (ou qu'on leur donne)

Beaucoup de faux positifs / faux négatifs

Efficaces pour les vulnérabilités "simples" (services exposés, versions vulnérables).

Pas toujours adaptés au Cloud / SaaS / Interne

Scans réseau classiques sont souvent inefficaces sur des environnements modernes (AWS, Azure, SaaS type M365).

Peu adapté aux audits authentifiés

Ne gèrent pas le multi-compte

Faibles en OSINT

Enumération dns, fuites, ASN, analyse certificats, archives web, recherche sites phishing

Pas d'autonomie/intelligence dans l'attaque

Pas de ré-utilisation des mots de passe fuités, pas de génération personnalisée (spraying attacks) -> pas de contexte

Peu exhaustifs / Très spécialisés

Obligation de multiplier les licences / outils pour être complets (mobile, interne web, etc.)

Peu de priorisation intelligente

Classe souvent par score cvss (pas de prise en contexte contexte métier, etc.)

STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Pentesteurs : Forces

Découverte de vulnérabilités complexes / métier

Logiques métiers, enchaînements d'actions, vulnérabilités "second order".

Audit en étant authentifié

Possibilité d'auditer une application avec un compte utilisateur / administrateur

Intelligence humaine

Efficaces pour les vulnérabilités "simples" (services exposés, versions vulnérables).

Vision offensive réaliste

Permet de comprendre l'angle d'attaque d'un adversaire.

Créativité humaine

Intuition + social engineering

Adaptabilité

Capable de s'adapter en fonction de la cible, techno, temps

Force pédagogique

Sensibilisation aux équipes, rapports priorisés

Test de résilience

Possibilité d'évaluer réaction du SOC, SIEM, équipe en condition réelle

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Pentests : limites

Dépendance aux compétences humaines

Qualité très variable pour selon le prestataire

Scope limité

Limité à quelques jours, difficiles sur les très gros périmètres

Effet bigbang

Gros rapports livrés en une fois

Côté humain, côté dispo

Pentest demande de la dispo : réunion kick-off, fourniture des accès, debriefs techniques

Coûts élevés

Difficilement soutenable pour des PME ou scans fréquents.

Pas toujours adapté au contexte

Trop "haut de gamme" pour des organisations peu matures.
Découvertes parfois peu actionnables (ex : injection SQL second order vs réalité → comptes faibles réutilisés).

Non scalable

Une équipe humaine ne peut pas couvrir 100% des actifs en continu.

Périodicité faible

Campagnes ponctuelles (annuelles/semestre), ne reflètent pas l'exposition quotidienne.

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Pentests : limites

OSINT limité

Pentesteurs pas toujours très focus sur l'osint (exception red team)

Prestations sur étagère

Ajouts devis si audit application mobile, veille fuites

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

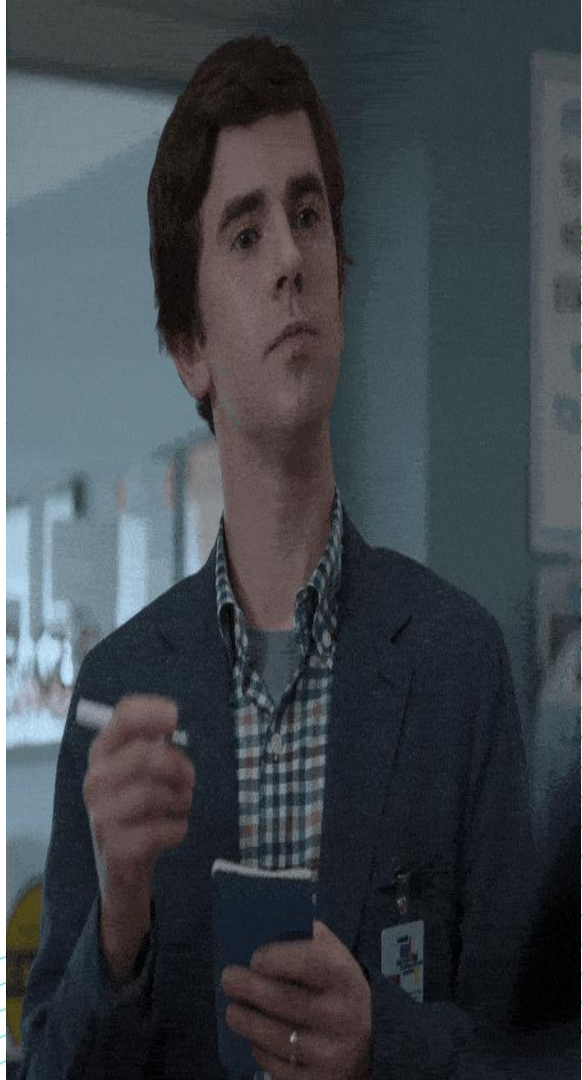
Constats

1. Limites actuelles des pentesteurs

- OSINT et fuites de données souvent sous-exploitées
- Pertes de temps par répétition des tâches manuelles
- Onéreux et peu scalables

2. Faiblesses des scanners de vulnérabilités

- Résultats trop génériques (beaucoup de bruit, peu de contexte)
- Portée limitée (pas d'OSINT, pas de fuites)
- Peu adaptés aux besoins MSSP (multi-clients, reporting valorisé)



© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Conclusion scanneurs de vulns et pentesteurs

Scanneur de vulns

Efficace pour **la surface technique de base**, mais insuffisant pour **une vision réaliste et contextuelle des risques**

Pentesteurs

Puissant et intelligent, mais souvent **trop coûteux, ponctuel et non scalable** pour couvrir les besoins de détection continue.

Peu de mix “pentest + scan” :

- PingCastle → trop passif
- Nessus/OpenVAS → trop généralistes

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

La vision Cyberesist

Un orchestrateur intelligent qui combine :

- 🕵️ OSINT + détection de fuites de données
- 🔎 Scans techniques enrichis et contextualisés
- ⚔️ Tests offensifs plus ciblés (greybox, AD, web, cloud)
- 📊 Rapports automatisés, visuels et “sexy” pour MSSP et RSSI

- Objectif : Combler le fossé entre pentesteurs humains et scanners automatisés.

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist : un mix entre un scanneur et un pentest

Fonctionnalités : niveau 1

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist : la plateforme d’audit « tout-en-un »

Idées

Un orchestrateur qui combine plus de 70 outils logiciels pour couvrir 2 offres :

- Audit de Surface d’Attaque Externe
- Audit de Réseau interne (AD CS & Azure)

Des processus 100% automatisés :

- Cartographie des systèmes
- Détection et analyse exhaustive des vulnérabilités
- Recommandations de solutions et Plans d’action
- Génération des rapports automatisée

Atouts et bénéfices

Très simple à utiliser

Des services s’adaptant aux périmètres audités

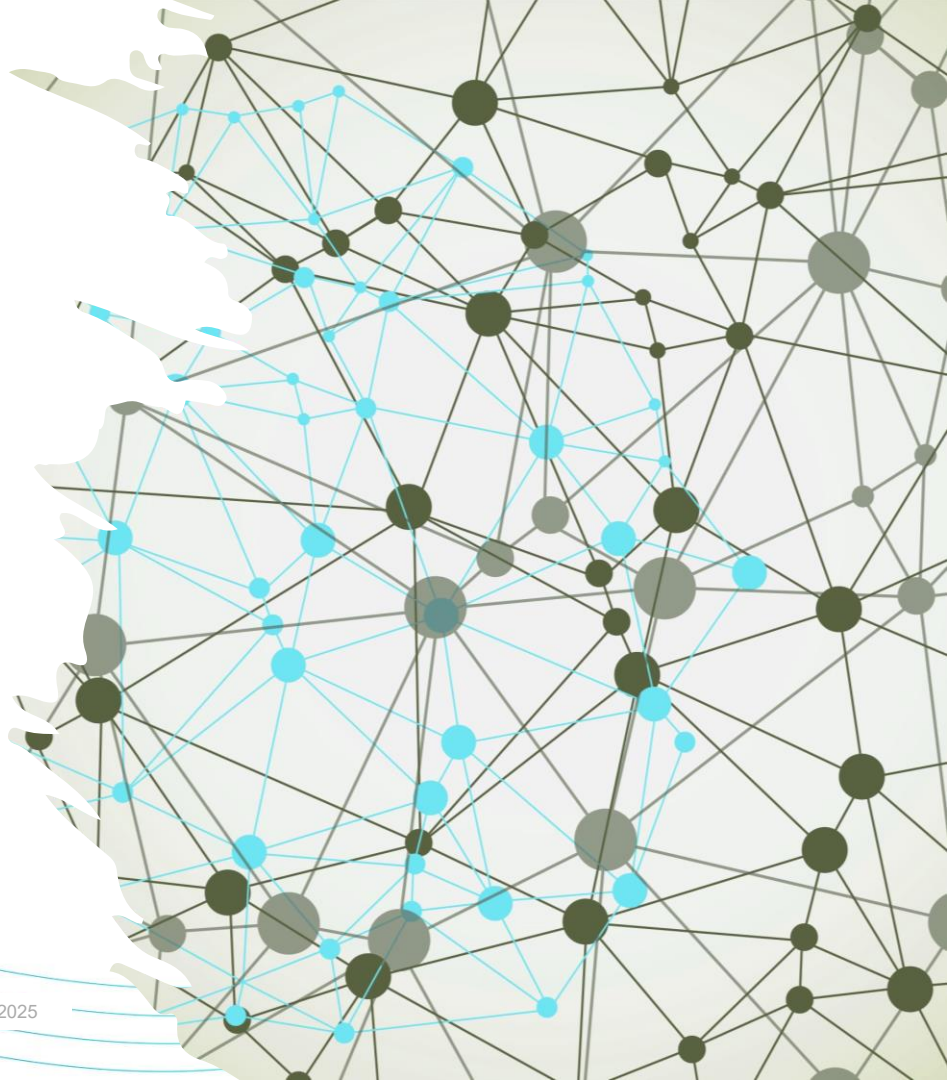
Architecture modulaire simplifiant les évolutions

Marque blanche pour nos partenaires

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist

Partie 1 : Web



© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist en mode scanneur de vulnérabilités web (niveau 1 auto)

Un peu plus fort en OSINT

Enumération dns, fuites, ASN, analyse certificats, archives web, recherche sites phishing, google dorks, github dorks

« Début d'intelligence »

Ré-utilisation des mots de passe découverts, Génération personnalisée (spraying attacks), Veille darkweb

All-in-one

Intégration de la partie scan de vulnérabilités + veille + attaques semi-automatisées

Large détection des applications

Wordpress, joomla, glpi, drupal, moodle, applications custom, etc.

Cyberesist en mode scanneur de vulnérabilités (web)

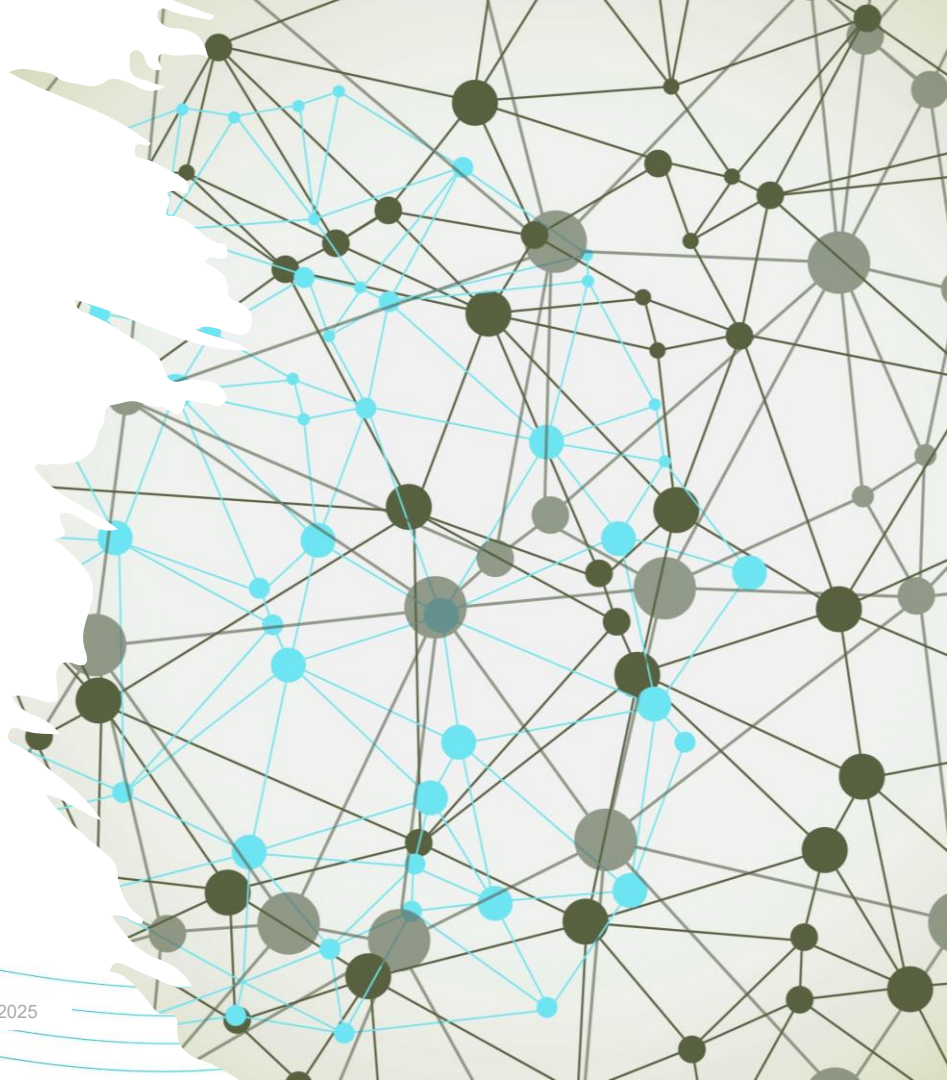
- Demo

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist

Partie 2 : audit interne

ACDS



© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Auditer son Active Directory / Entra-ID

Besoin d’auditer son Active Directory (ADCS ou Entra)

- Scanneur de vulnérabilités pas forcément hyper adaptés
  - Outil connu utilisé : Ping Castle

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist vs Ping Castle (ACDS) – Forces et faiblesses de PG

Analyse rapide et complète

Cartographie en quelques instants de l'état de sécurité de l'AD

Référence connue

Outil de facto pour auditer l'ad

Rapports clairs

Scoring global + recommandations

Bon indicateur de maturité

Permet aux équipes de se situer

Détection par les EDRs

Bloqué par de nombreux EDRS car utilisés lors d'attaques

Outil passif

Evalue la configuration et les risques, mais pas de tests plus « offensifs »

Couverture limitée

Teste uniquement l'AD, pas les stations de travail, ni le réseau

Usage payant en audit client

Licence impose une restriction .

Rapports non délivrables directement

Rapports html non délivrables directement au client

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist ADCS/Entra ID

Mix passif / offensif

Simulation de scénario d'attaque (~bloodhound), Analyse mots de passe dans répertoires partagés, test compte login/mdp, test pki, tests permissions, test esc privilèges en local etc.

Scan AD / réseau élargi

Découverte des services exposés, détection de services vulnérables au-delà de l'AD CS (exchange, sharepoint, etc.)

Audits postes de travail et serveurs

Détection mauvaises pratiques poste de travail (mots de passe dans navigateurs, présence edr / gestionnaire de mots de passe)

Couverture Cloud & Hybride

Vérification MFA, rôles globaux, owner applications, comptes invités, Secure Score

Rapport MSSP-ready

Rapports directement exportables pour le client. Pensé pour l'usage commercial

Rapidité

Effectué en quelques minutes

Utilisable en forensic (analyse de logs) et tests du SOC

Utilisateurs connectés, connexions depuis l'étranger, bruits

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist en mode scanneur de vulnérabilités (ADCS / Entra ID)

- Demo

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist : un mix entre un scanneur et un pentest

Fonctionnalités : Niveau 2

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Fonctionnalités niveau 2

- OSINT poussé (wayback archives + leaks + carto + fuzzing)
  - Récupération de vulnérabilités « introuvables » via scanneur classiques (profondeur limitée, etc)
  - Domaines non connus
  - Déterminer les points d'accès à fuzzer / auditer

```
http://marcl        /?action=FUZZ&module=FUZZ&order=FUZZ&orderby=FUZZ&page=FUZZ&
http://marcl        /index.php?AVIS.NICODE_SITE=FUZZ&action=FUZZ&module=FUZZ
http://marcl        /index.php?AVIS.NICODE_SITE=FUZZ&action=FUZZ&module=FUZZ&orc
http://marcl        /index.php?Provenance=FUZZ&action=FUZZ&module=FUZZ
http://marcl        /index.php?action=FUZZ
http://marcl        /index.php?action=FUZZ&module=FUZZ
http://marcl        /index.php?action=FUZZ&module=FUZZ&order=FUZZ&orderby=FUZZ
```

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Retour XP

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

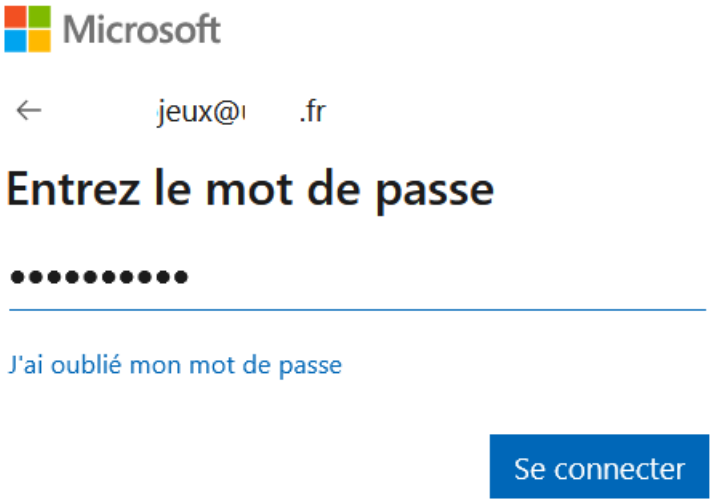
Retour XP

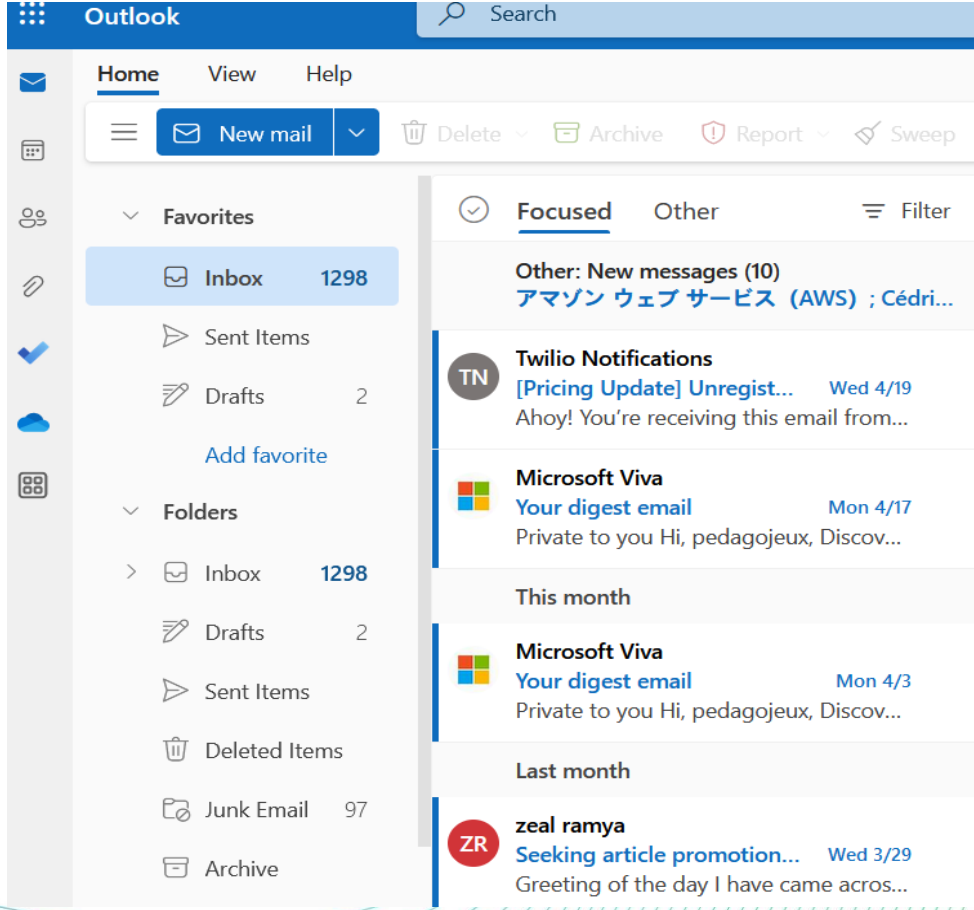
```
(venv) root@scw-clever-aryabhata-octo-backup:/artemisz/outils/osint/o365spray# python3 o365spray.py

          *** O365 Spray ***

>--------------------------------------<

   > version        :  2.0.4
   > domain         :
   > timeout        :  25 seconds
   > start          :  2023-04-26 14:32:15

>--------------------------------------<

[2023-04-26 14:32:15,452] INFO : Running O365 validation for:
[2023-04-26 14:32:15,598] INFO : [VALID] The following domain is using O365:  .fr
```

```
2023-04-26 14:36:58,661] INFO : Running O365 validation for:
2023-04-26 14:36:58,770] INFO : [VALID] The following domain is using O365:  .fr
2023-04-26 14:36:58,770] INFO : Running password spray against 1 users.
2023-04-26 14:36:58,771] INFO : Password spraying using paired usernames:passwords.
2023-04-26 14:36:59,222] INFO : [VALID]  jeux@  .fr:  jeux
2023-04-26 14:36:59,222] INFO :
```

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Retour XP





© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Fonctionnalités niveau 2

- Recherche et analyse auto applications Android
  - Recherche via google github / dorks
  - Récupération auto
  - Analyse via LLM et outils d'analyse statique
- Extraction automatisée .git / .svn + analyse via LLM

File is stored in an encrypted format on disk and cannot be read from or written to while the device is locked or booting.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-14
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Fonctionnalités niveau 2

- Audit ADCS scénarios d'attaque
  - Détection combinée : pas seulement une vulnérabilité isolée, mais des chaînes exploitables.
  - Cartographie offensive : mise en lumière de chemins réels d'escalade de privilèges.
  - Aide à la remédiation priorisée : démontrer l'impact concret pour convaincre le management

- Exemples de scénarios testés
  - LLMNR activé + Relais Kerberos
    - Capture de hash + relay sur un service ADCS vulnérable → certificat admin.
  - LDAP anonyme + Délégation de certificats mal configurée
    - Création d'un compte + demande de certificat → persistance.
  - Print Spooler actif + Accès RPC
    - Abus de PrintNightmare → pivot vers l'autorité de certification.
  - NTLMv1 autorisé + PKINIT mal configuré
    - Downgrade d'authentification → compromission Kerberos.
  - GPO contenant mot de passe en clair (cpassword) + ESC9
    - Extraction d'un compte privilégié → élévation via certificats

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Cyberesist : un mix entre un scanneur et un pentest

Fonctionnalités : Niveau 3

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Fonctionnalités niveau 3

- Analyse greybox d'applications web
  - Authentification automatique
  - Crawl post-login
  - Fuzzing IA ciblé (IDOR, LFI, Sqli, API, bypass logique)

- Objectifs :
  - Que peut vraiment faire un attaquant avec un identifiant récupéré ?
  - Approfondir les tests

Fonctionnalités niveau 3

- Récupération d'identifiants exposés (infostealer leaks, OSINT, pastebin, dark web, etc.) et rejeu automatisé
  - Identification login/pass/token/API key réels.
    - Plupart des scanners s'arrêtent aux surfaces anonymes.
  - Réutilisation intelligente d'identifiants (audit greybox).
    - Détection de l'interface web pour se connecter (via LLM)
    - Au lieu de scanner l'app en mode blackbox, connexion via un compte, un dashboard, une API authentifiée.
      - Surface exposée explose (admin panels, workflows, API internes, formulaires sensibles).
  - Couplage à un orchestrateur d'outils (Nuclei, SQLMap, Dalfox, etc.) mais après authentification.
  - Transformation des identifiants en vecteur d'attaque systématique.

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.

Perspectives

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préala

Le futur des audits / pentests

blogmoderateur 03/07/2025

🤖 L'IA est-elle déjà un meilleur pentester que l'humain ?

Sur HackerOne, l'une des principales plateformes de bug bounty au monde, un agent autonome baptisé XBOW a récemment atteint la première place du classement américain 🦾

Alors, faut-il s'inquiéter ou se réjouir ? Est-ce le signe d'un progrès spectaculaire dans la cybersécurité défensive ?

🎯 Overview

PentAGI is an innovative tool for automated security testing that leverages cutting-edge artificial intelligence technologies. The project is designed for information security professionals, researchers, and enthusiasts who need a powerful and flexible solution for conducting penetration tests.

© 2025 CYBERESIST
STRICTEMENT CONFIDENTIEL.
Ne pas copier, distribuer ou communiquer à des tiers sans autorisation écrite préalable.