Client: *carriereunion*

Rapport d'Évaluation de la Surface d’Exposition

Business Confidential

table des matières

Déclaration de Confidentialité

Ce document est la propriété exclusive de **Wilfridy Pentest** et **carriereunion.** Il contient des informations confidentielles et exclusives. Toute duplication, redistribution ou utilisation, en tout ou en partie, sous quelque forme que ce soit, requiert l'accord préalable des deux parties, **Wilfridy Pentest** et **carriereunion**

Wilfridy Pentest peut partager ce document avec des auditeurs sous accord de non-divulgation afin de démontrer la conformité aux exigences des tests d'intrusion.

Avertissement

Un test de pénétration est considéré comme une photographie de la sécurité du système à un moment donné. Les résultats et recommandations présentés reflètent les informations recueillies durant l'évaluation et ne tiennent pas compte des modifications ou changements effectués après celle-ci.

Les engagements à durée limitée ne permettent pas une évaluation complète de tous les contrôles de sécurité. Ainsi, **Wilfridy Pentest** a priorisé l'identification des contrôles de sécurité les plus vulnérables qu'un attaquant pourrait exploiter.

Wilfridy Pentest recommande de réaliser des évaluations similaires sur une base annuelle, soit en interne, soit par des assessors tiers, afin de garantir la pérennité et l'efficacité des contrôles de sécurité.

Aperçu de l'évaluation

Du 26 mars 2025 au 27 mars 2025, **Wilfridy Pentest** a été engagé par carriereunion pour effectuer une évaluation de la surface d'attaque de son infrastructure, en se concentrant uniquement sur la reconnaissance de surface, sans aller au-delà de cette phase. Cette évaluation n'inclut pas de test de pénétration complet, mais une analyse détaillée des informations accessibles de manière externe, sans exploitation des vulnérabilités.

Toutes les activités ont été menées selon les meilleures pratiques en matière de sécurité, en s'appuyant sur des méthodes adaptées à la reconnaissance de surface et les cadres de tests recommandés par le NIST SP 800-115 et l'OWASP Testing Guide (v4).

Les phases de la reconnaissance de surface incluent les suivantes :

1. **Planification** – Recueil des objectifs du client et des règles d'engagement.
2. **Découverte** – Réalisation de scans et d'énumérations pour identifier les informations accessibles publiquement et les éventuelles zones vulnérables de la surface d'attaque.
3. **Rapport** – Documentation des informations collectées, des points faibles identifiés et des recommandations générales pour sécuriser la surface d'attaque.

Composants de l'évaluation

Reconnaissance de Surface Externe

La reconnaissance de surface externe simule le rôle d'un attaquant tentant de collecter des informations accessibles publiquement afin d'évaluer la surface d'attaque d'un réseau interne, sans utiliser de ressources internes ni de connaissances privilégiées. Un ingénieur de **Wilfridy Pentest** effectue une collecte d'informations sensibles par intelligence en source ouverte (OSINT), incluant des informations sur les employés, des mots de passe compromis historiques, et d'autres données accessibles publiquement qui peuvent être utilisées pour analyser la surface d'attaque externe.

L'ingénieur procède également à des scans et des enquêtes pour identifier les points d'accès externes exposés et les éventuelles zones vulnérables pouvant nécessiter une attention particulière.

Scope

Évaluation	Détails
Surface Externe	Cumberland college

Exclusions du périmètre

À la demande de Cumberland college., **Wilfridy Pentest** n'a pas effectué d'attaques pendant l'évaluation de la reconnaissance de surface.

Autorisations du client

carriereunion autorise Wilfridy Pentest à effectuer une reconnaissance uniquement sur les domaines qui lui appartiennent et non sur ceux gérés par des tiers.

Résumé exécutif

Ce rapport présente les résultats d'une mission de reconnaissance de surface réalisée pour carriereunion. L'objectif de cette évaluation est d'identifier les actifs exposés sur Internet et de collecter des informations accessibles publiquement pouvant être exploitées par un attaquant lors d'une attaque plus avancée.

La reconnaissance de surface est une phase essentielle du test d'intrusion, permettant d'établir une cartographie des ressources visibles et d'évaluer le niveau d'exposition de l'organisation. Cette analyse inclut l'identification des noms de domaine, des adresses IP associées, des services accessibles, ainsi que des informations divulguées sur des sources publiques et des moteurs de recherche spécialisés.

Ce document détaille les méthodologies utilisées, les résultats obtenus et les recommandations pour réduire la surface d'attaque et limiter les risques de compromission.

Résumé de la reconnaissance de surface

Résumé de la reconnaissance de surface

Étape	Action	Recommandation

1	Collecte d'informations publiques : Exploration des domaines publics associés à carriereunion pour identifier les informations accessibles publiquement.	Limiter l'accès aux informations sensibles et effectuer des vérifications régulières des domaines associés.
2	Identification des services externes exposés : Analyse des services accessibles publiquement qui pourraient être exploités.	Restreindre l'accès aux services non nécessaires et les sécuriser correctement.
3	Analyse des sous-domaines : Vérification des sous-domaines associés à carriereunion et identification des sous-domaines potentiellement vulnérables et vérifier régulièrement et faire des mises a jours.	Limiter l'accès aux sous-domaines non utilisés et s'assurer qu'ils sont protégés correctement.
4	Analyse des informations de domaine : Vérification des informations de domaine pour s'assurer qu'elles sont à jour et renouvelées en temps voulu.	Vérifier régulièrement les informations de domaine et s'assurer qu'elles sont maintenues à jour.
5	Analyse des certificats SSL/TLS : Vérification des certificats SSL/TLS associés aux services externes pour garantir leur validité.	Mettre à jour les certificats SSL/TLS périodiquement pour maintenir la sécurité des services.
6	Analyse de la configuration réseau : Identification des ports ouverts sur les services externes.	Mettre à jour les configurations de sécurité et restreindre l'accès aux services non autorisés.

7	Analyse géographique des services : Vérification de la localisation des services externes pour détecter d'éventuelles vulnérabilités géographiques.	Limiter l'accès aux services à des régions géographiques nécessaires et sécuriser les services.

Résultats de la reconnaissance de surface externe

Description :
carriereunion a des informations sensibles facilement accessibles publiquement, telles que des adresses IP, des sous-domaines et des adresses e-mail. Cette exposition constitue une surface d'attaque potentielle qui pourrait être exploitée par des attaquants pour réaliser des attaques de phishing, de force brute ou d'autres tentatives d'intrusion.

Impact :
Critique – Ces informations sont facilement accessibles et pourraient être utilisées pour mener des attaques externes contre l'infrastructure de carriereunion

Système :

Domaines et sous-domaines détectés :

- INF] Current subfinder version v2.6.0 (outdated)
- [INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
- [INF] Enumerating subdomains for carriereunion.com
- extranet.carriereunion.com
- cpcalendars.carriereunion.com
- www.carriereunion.com
- webmail.carriereunion.com
- carriereunion.com
- cpanel.carriereunion.com
- cpcontacts.carriereunion.com
- mail.carriereunion.com
- webdisk.carriereunion.com
- www.extranet.carriereunion.com
- [INF] Found 10 subdomains for carriereunion.com in 718 milliseconds 748 microseconds

NF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for carriereunion.ca

carriereunion.ca
www.carriereunion.ca
[INF] Found 2 subdomains for carriereunion.ca in 5 seconds 24 milliseconds

- Adresses IP identifiées :
  - 24.37.42.94
  - 204.191.10.64
    216.172.184.173

Preuve de Concept

Bien qu'aucune exploitation directe des vulnérabilités n'ait été réalisée, Wilfridy Pentest a identifié plusieurs points de vulnérabilité potentiels à travers la collecte d'informations accessibles publiquement. Les informations suivantes ont été recueillies :

1. **Domaines et sous-domaines** exposés publiquement.
2. **Adresses e-mail** visibles : contact@carriereunion.com, info@carriereunion.com.
3. **Adresses IP** publiques associées aux services externes de carriereunion.com : 216.172.184.173

Ces informations exposent carriereunion.com. à des risques d'attaques par phishing, force brute ou exploitation de services externes non sécurisés.

Remédiation

Qui:	Équipe IT de Cumberland college
Actions recommandées :	▪ **Exposition des informations publiques :** Wilfridy Pentest recommande à carriereunion de limiter l'accès public aux informations sensibles telles que les sous-domaines, adresses IP et adresses e-mail. ▪ **Mise à jour des configurations réseau :** o Restreindre l'accès aux sous-domaines non nécessaires (par exemple, eu.carriereunion, cpanel.carriereunion). o Limiter l'exposition des adresses IP publiques et restreindre l'accès aux IP inutiles. ▪ **Renforcement des mesures de sécurité :** o S'assurer que les services externes sont correctement sécurisés et que les certificats SSL/TLS sont à jour. o Restreindre l'accès aux informations publiques et périodiquement vérifier les configurations de sécurité des services exposés. ▪ **Sensibilisation des employés :** o Former les employés sur la gestion des mots de passe et sur la création de mots de passe robustes. o Vérifier les informations de connexion des employés contre des bases de données de mots de passe compromis pour éviter l'utilisation de mots de passe faibles ou compromis.

Rapports et Informations supplémentaires (Informative)

Wilfridy Pentest fournit à ses clients toutes les informations collectées lors de l'évaluation. Cela inclut les données obtenues lors de la reconnaissance de surface et un rapport détaillé des conclusions. Pour plus d'informations, veuillez consulter les documents suivants:

- **carriereunion_TheHarvester.pdf**
- **carriereunion_Recon-ng.pdf**
- **Carriereunion _Whois.pdf**
- **carriereunion _crt.sh.pdf**
- **carriereunion _Shodan.pdf**
- **carriereunion _Nmap.pdf**