

MISSION EXTERNE ET INTERNE · INDUSTRIE LOURDE

D'une application exposée sur Internet à la prise de contrôle totale du domaine

Un groupe industriel lourd de la région du Golfe

Anonymisée avec l'accord écrit du client. Organisation, systèmes, noms d'hôtes, adresses, comptes et tout autre identifiant présents dans le rapport d'origine ont été supprimés ou généralisés. Les vulnérabilités sont décrites de manière à ne pas permettre de remonter au client.

Client	Un groupe industriel lourd (anonymisé)
Mission	Test d'intrusion externe des systèmes exposés sur Internet, prolongé par un audit interne de l'Active Directory
Approche	Approche grey-box, sur deux semaines environ, à distance depuis une adresse IP source fixe
Testeur	Ismail Regragui, Vallum Security · OSCP, OSEP, BSCP, OSWP · Synack Red Team
Référentiels	OWASP WSTG, OWASP API Security Top 10, NIST SP 800-115 ; gravité selon CVSS v3.1

La demande

Tester les applications web exposées sur Internet ainsi que les services de messagerie et d'accès distant, puis, à partir d'un simple compte de domaine peu privilégié, mesurer jusqu'où un attaquant pouvait progresser dans l'Active Directory interne.

Vue d'ensemble



Vulnérabilités en un coup d'œil

ID	VULNÉRABILITÉ	GRAVITÉ
----	---------------	---------

1	Exécution de code à distance non authentifiée via un web shell dormant sur un serveur applicatif public	Critique
2	Compromission complète du domaine Active Directory depuis un simple compte utilisateur	Critique
3	Comptes de service à hauts privilèges vulnérables au cassage de mot de passe hors ligne (Kerberoasting)	Élevée
4	Énumération de comptes et réinitialisation de mot de passe mal protégée sur un portail en libre-service	Élevée
5	Énumération de comptes depuis une page de connexion publique	Moyenne
6	Protection anti-force brute insuffisante sur le webmail, contournable par pulvérisation de mots de passe (password spraying)	Moyenne
7	Rapport d'un outil de build laissé accessible au public, révélant la structure interne de l'application	Moyenne
8	Contrôle des fichiers appliqué au téléchargement mais pas à l'envoi	Moyenne
9	Composant d'interface tiers obsolète visé par des exploits publics (non exploitable ici grâce à des mesures compensatoires)	Faible

Les vulnérabilités sont renumérotées et reformulées pour cette étude de cas. Noms d'hôtes, chemins, comptes et adresses du rapport d'origine ont été retirés.

Chaîne d'attaque principale : du serveur web public au contrôle du domaine

Les deux vulnérabilités critiques se sont enchaînées en un seul chemin, d'Internet jusqu'au contrôle complet du domaine.

- 1. Point d'entrée.** L'énumération de contenu sur un serveur applicatif public a mis au jour un script non standard, oublié là depuis des années. Il exécutait des commandes sans authentification, offrant un accès immédiat au serveur Windows sous-jacent.
- 2. Récupération d'identifiants.** Cet accès donnait à lire des fichiers de configuration où figuraient, en clair, des identifiants de base de données et de comptes de service. En parallèle, un portail en libre-service permettait d'énumérer une série de comptes internes en indiquant lesquels existaient.
- 3. Bascule vers l'interne.** Depuis un simple compte de domaine peu privilégié, l'environnement interne a été cartographié. Un compte applicatif disposait de droits bien plus étendus que prévu, dont le contrôle de plusieurs serveurs sensibles.
- 4. Élévation de privilèges.** Ces droits excessifs, combinés à des sessions d'administrateurs privilégiés laissées ouvertes sur des serveurs ordinaires et à l'absence de durcissement, ont permis — via un abus de délégation classique — d'obtenir les droits de Domain Admin.

5. **Impact.** Dès lors, l'ensemble des serveurs, postes et comptes du domaine devenait accessible, y compris des systèmes hébergeant des documents commerciaux sensibles.

Supprimer ce script oublié, ou corriger ce seul compte aux droits surdimensionnés, aurait suffi à rompre la chaîne — deux correctifs peu coûteux au regard du risque.

Ce qui fonctionnait bien

- ✓ La protection des postes (antivirus/EDR) a bloqué plusieurs tentatives d'élévation et contraint à des techniques plus discrètes, menées à la main.
- ✓ Le TLS était correctement configuré sur les services publics testés.
- ✓ Les accès aux bases de données reposaient sur des requêtes paramétrées : aucune injection SQL n'a été trouvée sur les applications testées.

Axes de remédiation

- Retirer les fichiers inconnus ou hérités des racines web et considérer le serveur concerné comme compromis : le reconstruire à partir de sources saines et renouveler tous les identifiants exposés.
- Réduire au strict minimum les appartenances aux groupes privilégiés et les droits de délégation, et tenir les comptes d'administration à l'écart des serveurs courants (administration en tiers).
- Activer les protections des identifiants sur les serveurs et les contrôleurs de domaine, et migrer les comptes de service vers des comptes gérés, à rotation automatique.
- Ajouter limitation du nombre de tentatives, messages d'erreur uniformes et authentification multifacteur sur tous les flux de connexion et de réinitialisation exposés sur Internet.

Résultat. Toutes les vulnérabilités critiques et élevées ont été recontrôlées après correction et confirmées résolues ; le client a reçu un rapport mis à jour et une attestation pour ses auditeurs.