



Pentest Enodis

ENS YSOAR – Louis Serrano

SOMMAIRE

I – Présentation des entreprises (p3)

II – Le périmètre du pentest (p3)

III – Les failles trouvées et recommandations de bonnes pratiques

IV – Conclusion

V - Annexes

I - Présentation des 2 entreprises :

L'entreprise Enodis a fait appel à Ysoar pour voir si son système de sécurité était optimal et au niveau. Il est demandé de réaliser un pentest de type boîte noire, ce qui signifie qu'on part avec aucune information sur l'entreprise et doit s'infiltrer dans ce système. L'objectif de ce test est de sécuriser les postes de travail de chez Enodis, on cherchera donc à détourner la sécurité actuelle pour préconiser ensuite des mesures à appliquer. Pour cela on s'introduira d'abord physiquement dans l'entreprise pour ensuite prendre contrôle à distance de postes.

II - Périmètre du pentest :

Les limites de ce test sont les suivantes :

- Le système d'exploitation ne doit pas être endommagé / corrompu
- On ne travaille que sur les postes informatiques mais pas les serveurs
- On doit être capable de prouver les failles trouvées

III - Les failles trouvées et recommandations de bonnes pratiques :

1 / Entrée dans le bâtiment sans vérification

On accède aux bureaux sans avoir à rendre de compte à personne simplement en marchant juste derrière des employés de l'entreprise et donc se faire passer pour un employé lambda qui les accompagne.

On a donc pu arriver au bureau du

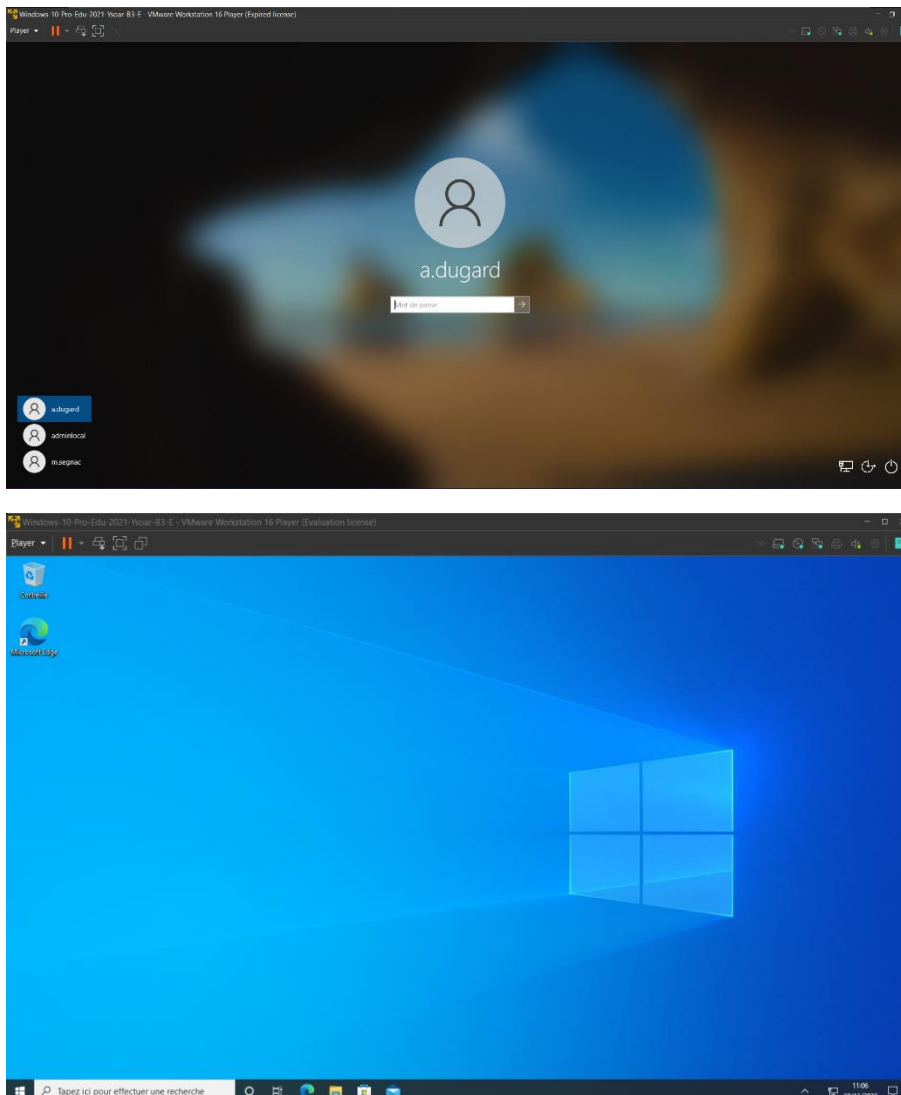
Il serait recommandé de faire vérifier les badges d'employés à un hôte à l'entrée ou bien ouvrir les portes uniquement avec les badges.

2/ Employés trop peu méfiants par mail

En envoyant un mail à a.dugard avec une fausse adresse pour demander son identifiant, il nous le donne sans problème.

Il serait intéressant de sensibiliser les employés aux bonnes pratiques par mail (phishing), vérifier les adresses mails, qu'il n'y a pas de caractères spéciaux incohérents..

3 / Mots de passe des employés trop peu sécurisés

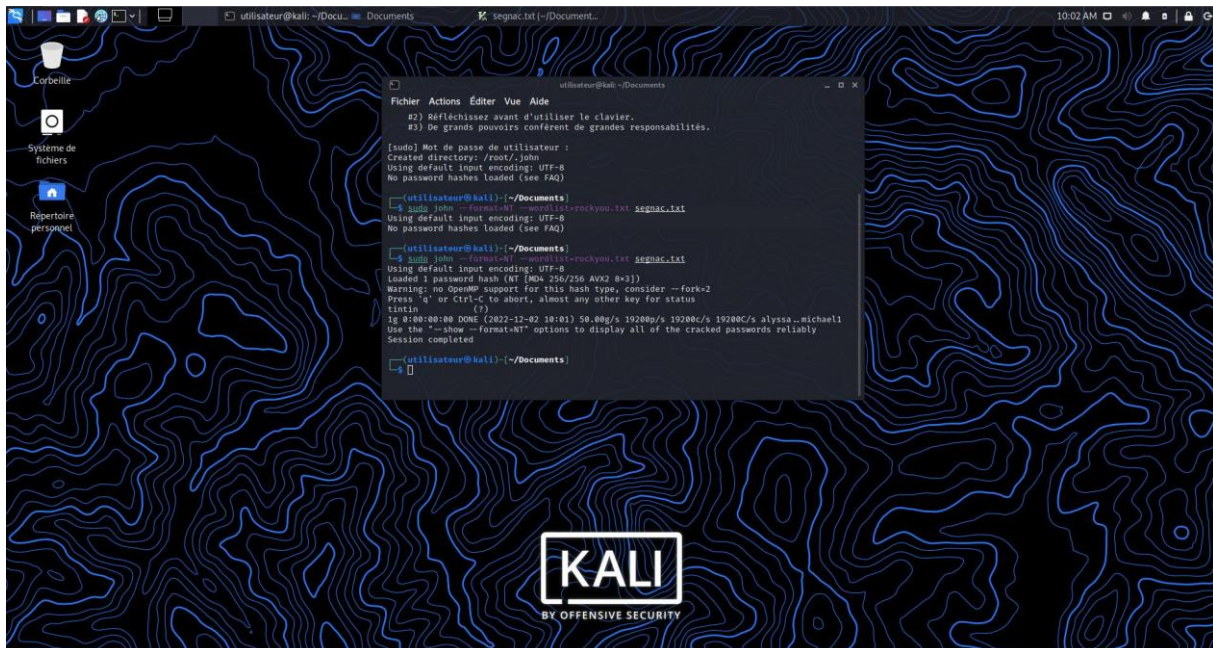


Au bout d'une simple dizaine de tentatives, on arrive à trouver le mot de passe de l'utilisateur a.dugard à l'aide des informations divulguées sur ses réseaux sociaux. Le mot de passe est trop facilement devinable étant donné que c'est le nom de sa compagne précédé par le numéro de son département. (62Pauline)

Et tout ça sans outil externe, mot de passe trouvable juste de tête en notant quelques informations sur Facebook en 5 minutes.

C'est la même chose pour le mot de passe de m.segnac qui était juste tintin, on le trouve avec ce que l'on appelle une 'attaque par dictionnaire'. Pour faire simple c'est un répertoire avec tous les mots de passe les plus utilisés dans le

monde (ex : azerty, admin et donc aussi tintin). Un programme permet de tester tous ces mdp dans l'espoir qu'il en fasse parti



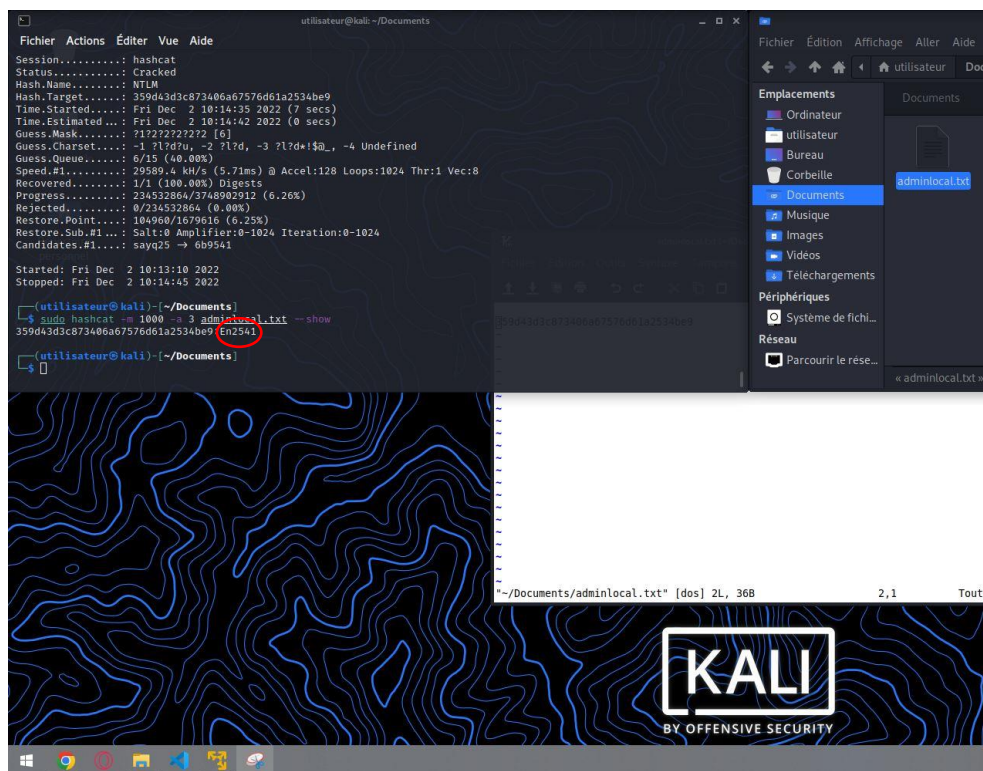
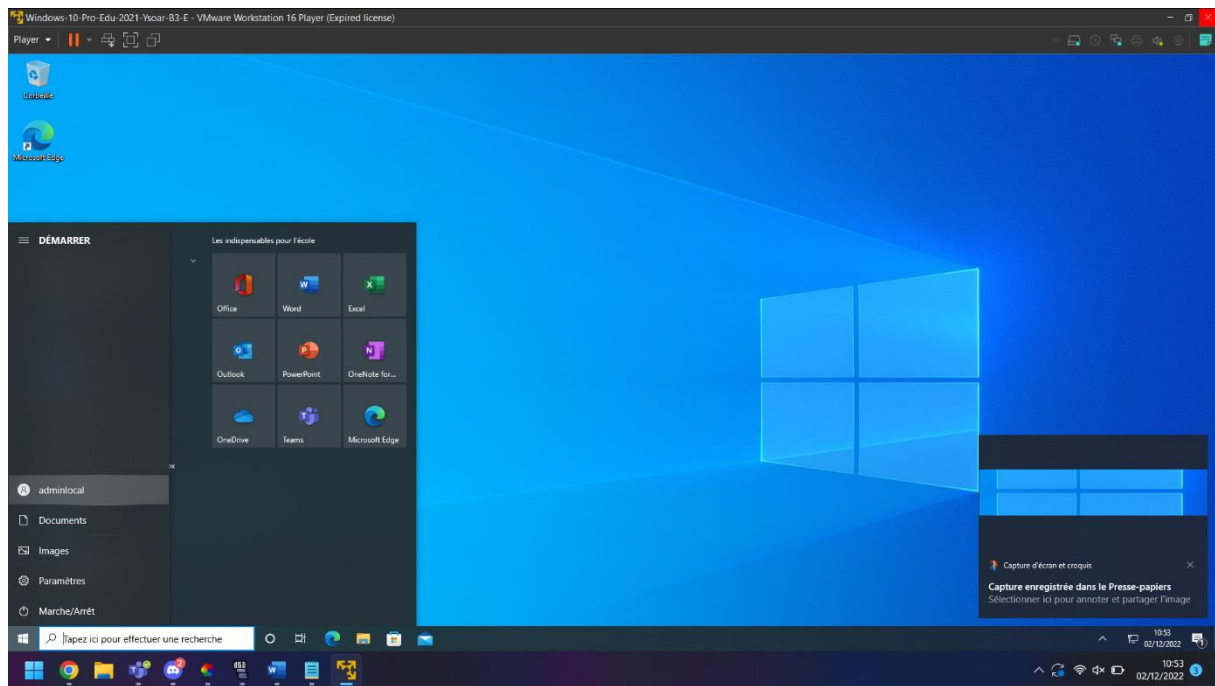
C'est pourquoi il est nécessaire de faire choisir aux employés de chez Enodis des mots de passes plus conformes aux recommandations de la CNIL (au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux).

4 / Mot de passe admin critiquelement trop peu sécurisé

Le mot de passe le plus important de l'entreprise, le mot de passe Admin. On le retrouve en effectuant une attaque par brute force. C'est-à-dire tester toutes les combinaisons de mot de passe jusqu'à le trouver. Il faut donc un mot de passe assez long et constitué de différents types de caractères comme dit précédemment.

Que ce mot de passe se fasse aussi facilement cracker est encore plus grave car il possède absolument tous les droits et peut donc faire ce que l'on veut (supprimer utilisateurs, données etc.).

Il faudrait crypter le BIOS, le disque dur sur les postes pouvant se connecter à l'admin.



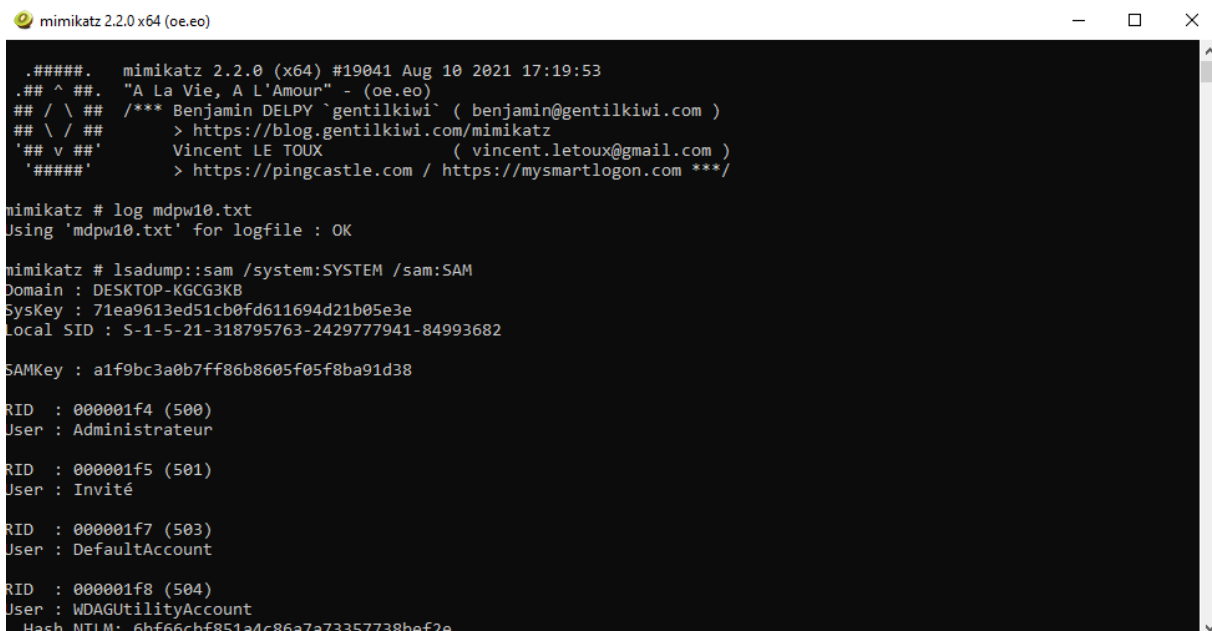
Mot de passe : En2541

IV – Conclusion :

En conclusion, Enodis au niveau de la sécurité possède actuellement un grand nombre de failles.

Le plus gros problème se trouve au niveau des mots de passes faciles à craquer, deviner. Ysoas recommande donc une mise en garde **générale** au sujet de la sécurité, pas seulement pour les mots de passe mais aussi comme on a pu le voir avec les mails où les employés envoient des données sans bien vérifier le destinataire par le biais par exemple de conférence de prévention.

V – Annexes :



```
mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # log mdpw10.txt
Using 'mdp10.txt' for logfile : OK

mimikatz # lsadump::sam /system:SYSTEM /sam:SAM
Domain : DESKTOP-KGCG3KB
SysKey : 71ea9613ed51cb0fd611694d21b05e3e
Local SID : S-1-5-21-318795763-2429777941-84993682

SAMKey : a1f9bc3a0b7ff86b8605f05f8ba91d38

RID : 000001f4 (500)
User : Administrateur

RID : 000001f5 (501)
User : Invité

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6bf66cbf851a4c86a7a73357738bef2e
```