

[Énumération] Samba

Introduction

L'énumération des partages samba est cruciale pour les tests d'intrusions d'environnement Windows.

Script nmap

Énumération globale de l'OS utilisé

```
nmap --script smb-os-discovery <IP>
```

Énumération des utilisateurs samba

```
nmap --script smb-enum-users <IP>
```

Cette technique ne marche que si la session "**null**" est activée sur le poste cible (rare).

Smbmap

Utilisation avec un compte

Si vous possédez un compte pour faire l'énumération :

```
smbmap -u <USER> -p <PASSWORD> -H <IP>
```

Vous aurez un aperçu des droits de lecture et d'écriture que vous avez sur les partages.

Utilisation de la session null

```
smbmap -u "" -p "" -H <IP>
```

Options

Options	Descriptions
-R	Active la récursivité pour afficher le contenu des dossiers (si vous possédez les droits de lecture).

ShareEnum

Installation

Vous pouvez récupérer la dernière release sur le [github](#) et lancer l'installation du paquet sur votre système :

```
dpkg -i <PACKAGE>.deb
```

Utilisation standard

```
shareenum <IP>
```

Si vous ne spécifiez pas d'utilisateur, la session **null** sera utilisée.

Options

Options	Descriptions
-o <FILE>	Spécifie un fichier de sortie de la commande.
-u <USER>	Spécifie un nom d'utilisateur.
-p <PASSWORD>	Spécifie un mot de passe.

SMBClient

On peut énumérer tous les fichiers d'un partage avec **smbclient** :

```
smbclient -N //<IP>/<SHARE>
```

Revision #3

Created 10 November 2023 13:59:08 by Elieroc

Updated 3 May 2024 14:28:42 by Elieroc