DE LA RECHERCHE À L'INDUSTRIE

accenturesecurity

manwefm/ipfyx

membre fondateur 2016

manwefm

Bureau 2016

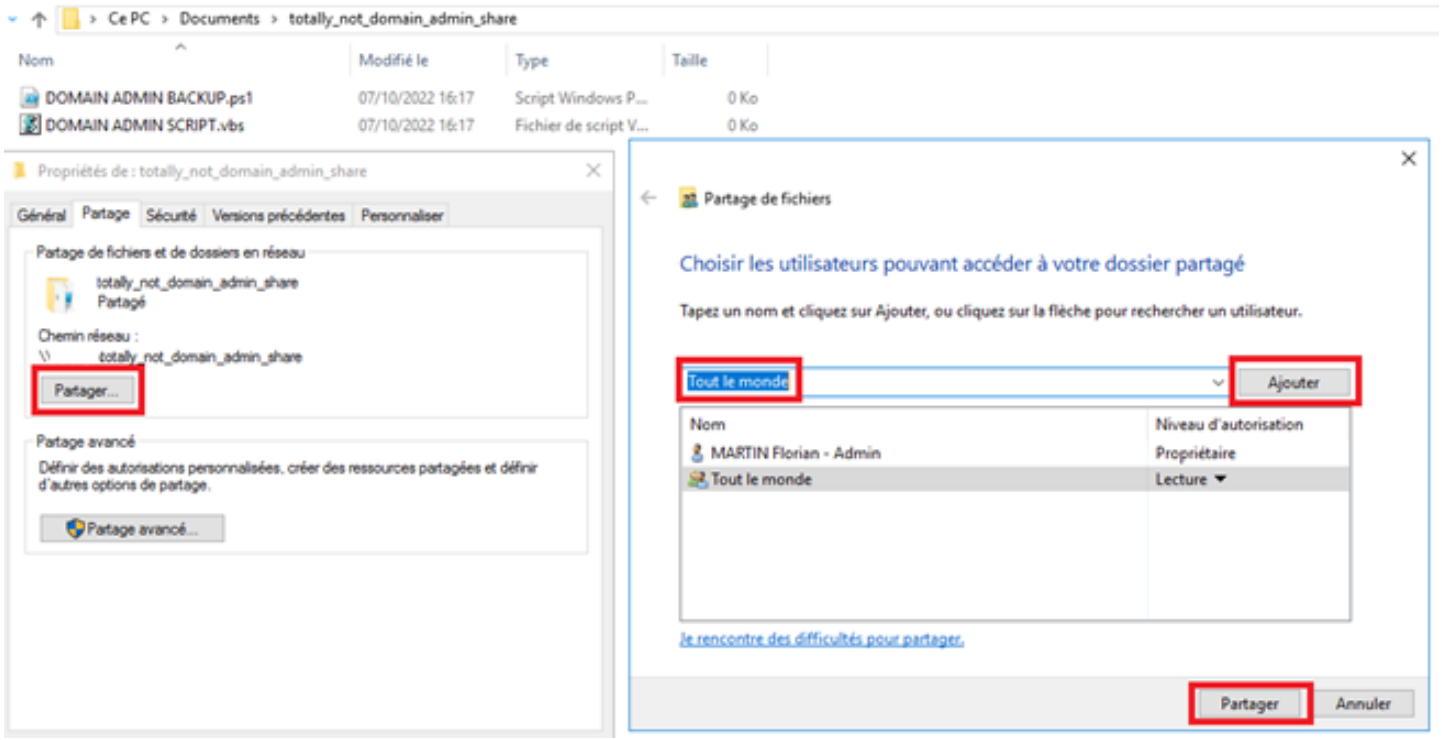
Blueteam vs SMB

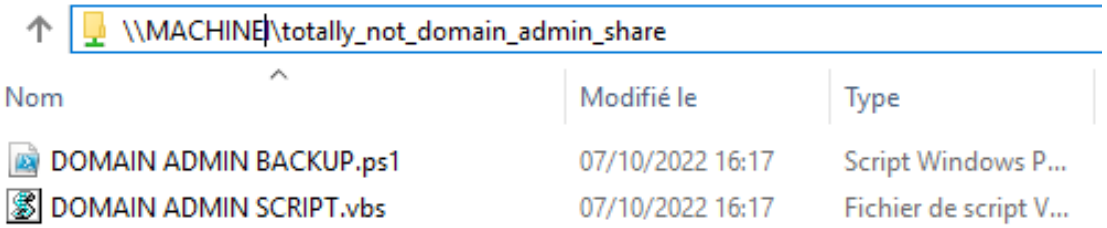
11 octobre 2022

Florian MARTIN : SOC/CSIRT

Partager un dossier sur Windows : easy

- Read ou FullControl Everyone ?





Comment les trouver ? Par scans réseaux ?

	Nmap + NSE scripts
Âge	NSE : 2008 - 2015
SMB v1	✓ PR #2301
SMB v2 et v3	✘
MetaData[1]	✓
Droits précis ?	READ|READ_WRITE
Fait le café	✘

- **Limites : filtrages réseaux**

[1] Version des protocoles supportées, SMB signing etc.

Comment les trouver ? Par scans réseaux ?

	Nmap + NSE scripts	smbclient
Âge	NSE : 2008 - 2015	01/01/1970 ?
SMB v1	✓ PR #2301	✓
SMB v2 et v3	✗	✓
MetaData[1]	✓	✗
Droits précis ?	READ|READ_WRITE	READ|READ_WRITE
Fait le café	✗	✗

- **Limites : filtrages réseaux**

[1] Version des protocoles supportées, SMB signing etc.

Comment les trouver ? Par scans réseaux ?

	Nmap + NSE scripts	smbclient	PowerHuntShares[2]
Âge	NSE : 2008 - 2015	01/01/1970 ?	04/2022
SMB v1	✓ PR #2301	✓	✓
SMB v2 et v3	✗	✓	✓
MetaData[1]	✓	✗	✓
Droits précis ?	READ|READ_WRITE	READ|READ_WRITE	FULL SDDL
Fait le café	✗	✗	✓

- **Limites : filtrages réseaux**

[1] Version des protocoles supportées, SMB signing etc.

[2] https://www.netspi.com/blog/technical/network-penetration-testing/network-share-permissions-powerhuntshares

Logs Windows : event 5143 - un objet de partage réseau a été modifié

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'audit	07/10/2022 16:34:49	Microsoft Windows security auditing.	5143	Partage de fichiers
Succès de l'audit	07/10/2022 16:34:03	Microsoft Windows security auditing.	5143	Partage de fichiers

Événement 5143, Microsoft Windows security auditing.

Général | Détails

Un objet du partage réseau a été modifié.

Sujet :
- ID de sécurité : HACKADEMINT\A-FLORIAN
- Nom du compte :
- Domaine du compte :
- ID d'ouverture de session : 0x52132843

Informations sur le partage :
- Type d'objet : Directory
- Nom de partage : *\totally_not_domain_admin_share
- Chemin d'accès du partage : C:\Users\ \Documents\totally_not_domain_admin_share
- Remarque précédente : N/A
- Nouvelle remarque : N/A
- Nombre maximal d'utilisateurs précédent : 0xFFFFFFFF
- Nouveau nombre maximal d'utilisateurs : 0xFFFFFFFF
- Indicateurs de partage précédents : 0x0
- Nouveaux indicateurs de partage : 0x0
- Ancien SD : O:BAG:S-1-5-21- D:(A;;0x1200a9;;;WD)
- Nouveau SD : O:BAG:S-1-5-21- D:(A;;FA;;;WD)

Quand et Qui

A partagé

Quoi et Où

Et

Comment ?

ACL[1] & SDDL[2]

Sddl : …(A;;FA;;;WD)(sddl2)(sddl3)…

(A;;FA;;;WD) ≈ chmod 777

A : Allow

FA : Full Access

WD : Wolrd (Everyone)

Acronyme	Nom
AN	Anonymous logon
AU	Authenticated Users
BU	Builtin- Users
DC	Domain Computers
DU	Domain Users
WD	**Everyone**
LG	Local Guest
BG	Built-in Guest

[1] Access Control List
[2] Security Descriptor Definition Language

```
PS C:\> Get-Acl \\[redacted]\totally_not_domain_admin_share|fl

Path   : Microsoft.PowerShell.Core\FileSystem::\\[redacted]\totally_not_domain_admin_share
Owner  : [redacted]
Group  : [redacted]\Domain Users
Access : Tout le monde Allow  ReadAndExecute, Synchronize
         AUTORITE NT\Système Allow  FullControl
         BUILTIN\Administrateurs Allow  FullControl

Audit  :
Sddl   : O:S-1-5-21 G:DUD:AI (A;OICI;0x1200a9;;;WD)(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)
```

Comment les trouver ? Par les logs ?

```
1 index=adlogs 5143 totally_not_domain_admin_share event_id=5143
2 | search (AN OR AU OR BG OR BU OR DC OR DG OR DU OR WD OR LG)
3 OR (TERM("S-1-5-7") OR TERM("S-1-5-11") OR TERM("S-1-5-546") OR TERM("S-1-5-545") OR TERM("S-1-5-*-515") OR TERM("S-1-5-*-514") OR TERM("S-1-5-*-513") OR TERM("S-1-1-0") OR TERM("S-1-5-*-501"))
4 NOT (LocalSplOnly OR print OR prnproc)
5 | stats min(_time) as time_min, max(_time) as time_max count as occurence last(NewSD) as NewSD values(OldSD) as OldSD by host, SubjectUser, SubjectDomain, ShareLocalPath, ShareName
6 |eval time_min=strftime(time_min, "%d/%m/%Y %H:%M:%S"),time_max=strftime(time_max, "%d/%m/%Y %H:%M:%S")
7 | search NewSD IN ("*WD*","*AN*","*AU*","*BU*","*DU*","*DC*","*S-1-5-7*", "*S-1-5-11*","*S-1-5-546*", "*S-1-5-545*", "*S-1-5-*-515*", "*S-1-5-*-514*", "*S-1-5-*-513*", "*S-1-1-0*", "*S-1-5-*-501*")
```

Last 24 hours

✓ **2 events** (06/10/2022 18:00:00.000 to 07/10/2022 18:47:08.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (1)** Visualization

100 Per Page Format Preview

host	SubjectUser	SubjectDomain	ShareLocalPath	ShareName	time_min	time_max	occurence	NewSD	OldSD
[redacted]	[redacted]	[redacted]	C:\Users\A-[redacted]\Documents\totally_not_domain_admin_share	*\totally_not_domain_admin_share	07/10/2022 16:34:03	07/10/2022 16:35:10	2	O:BAG:SI-513D:(A;;FA;;;WD)	O:BAG:SI-513D:(A;;0x1200a9;;;WD) O:BAG:SI-513D:(A;;FA;;;WD)

- Recherche plaintext
- Sans regex

- Limites : Linux, Isilon etc. car logs différents

Et hop plus de SMB !

Acronyme	Nom
AN	Anonymous logon
AU	Authenticated Users
WD	Everyone

- **Y a plus**