

Challenge SSTIC 2026 - Step 5 : dumping through my screen

nebucca

Analyst,

Thanks for the database! At this point, you have all the informations needed to disable SAFE. We will continue to monitor the situation while you disable the system.

It may be a little early, but thanks for helping us handle this crisis.

-ñ

1 Extraction de la base

Nous sommes maintenant capables de parcourir l'intégralité de la base de données... via une sortie vidéo.

Donc, première étape, trouver les bons outils pour transformer ce flux en données.

Complicé mais la combinaison gagnante pour moi fut :

- script pour automatiser le parcours de la base de données,
- *OBS Studio* pour enregistrer l'affichage des données,
- *VideOCR* pour convertir la vidéo en texte,
- extraction des séries hexadécimale,
- régénération du fichier d'origine.

Fastidieux de trouver les bons réglages mais finalement la base est là.

2 Recherche du chemin

La structure des enregistrements est relativement simple :

Offset	Taille	
0x0	0x40	Username
0x40	0x4	Droits
0x44	0x20	Hash du password
0x64	0x8	Nb groupes
0x6c	0x8	ID Groupe

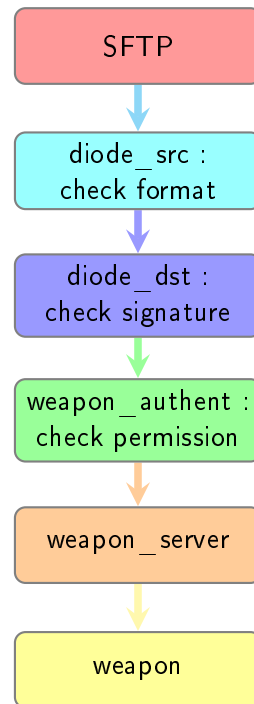
En regardant les droits des différents utilisateurs, on se rend compte que l'utilisateur qui a le plus de droits est *audit_KaKaHuet*.

Il est temps de faire appel aux messages d'impersonnification : un utilisateur peut impersonnifier un autre utilisateur s'ils ont un groupe en commun.

L'idée est donc de trouver un chemin entre *SSTIC_USER* et *audit_KaKaHuet* en passant par des utilisateurs intermédiaires ayant des droits suffisants pour réaliser une impersonnification, et un groupe commun permettant de passer de l'un à l'autre.

Afin de ne pas trop allonger le chemin, on part sur un algorithme de parcours BFS. Le chemin est vite trouvé.

Il ne reste plus qu'à envoyer les différents messages pour obtenir les droits de *audit_KaKaHuet*, et à envoyer un dernier message qui sera transmis à la partie *weapon* via les pipes.



Voilà. :)

```
sstic-69866ad8a886-sstic-challenge-diode-dest-6965b6f686-t49cp:1 - TigerVNC
Master Secure Terminal

weapon server
mail: /log/weapon_server.log: file truncated

System disarmed. Thank you for participating in this year cyber awareness for
contractors exercise. Mail us @
System disarmed. Thank you for participating in this year cyber awareness for
contractors exercise. Mail us @
System disarmed. Thank you for participating in this year cyber awareness for
contractors exercise. Mail us @
777a6c006a0f848986e7420e3210640734535648ee507d0cc10d5d434314cc96@sstic.org -
Sivi

diode dest.log
0000 1e49d042 06-00-00-00-01-00-00-02-6F-6B .....ok
end:1E49D042
=====
05-14 14:23:34 - [INFO] processing message WEAPONS_MSG

=====
resp:00C8
0000 abf9cee9 04-00-00-00-01-00-00-C0-53-79-73-74-65-6D-20-64 .....System d
0010 9ca4401d 69-73-61-72-6D-65-64-2E-20-54-68-61-6E-6B-20-79 isarmed. Thank y
0020 56f7db6c 6F-75-20-66-6F-72-20-70-61-72-74-69-63-69-70-61 ou for participa
0030 41f64e65 74-69-6E-67-20-69-6E-20-74-68-69-73-20-79-65-61 ting in this yea
0040 8ec15f6b 72-20-63-79-62-65-72-20-61-77-61-72-65-6E-65-73 r cyber awarenes
0050 215093f1 73-20-66-6F-72-20-63-6F-6E-74-72-61-63-74-6F-72 s for contractor
0060 0d2b1719 73-20-65-78-65-72-63-69-63-65-2E-20-4D-61-69-6C s exercice. Mail
0070 543eac8b 20-75-73-20-40-20-37-37-61-36-63-30-30-36-61 us @ 777a6c006a
0080 766b52ef 30-66-38-34-38-39-38-36-65-37-34-32-30-65-33-32 0f848986e7420e32
0090 50ca9e36 31-30-36-34-30-37-33-34-35-33-35-36-34-38-65-65 10640734535648ee
00a0 ea265bd4 35-30-37-64-30-63-63-31-30-64-35-64-34-33-34-33 507d0cc10d5d4343
00b0 ae76b856 31-34-63-63-39-36-40-73-73-74-69-63-2E-6F-72-67 14cc96@sstic.org
00c0 e84c29cb 20-2D-20-53-69-76-69-00- - Sivi.
end:40483C9E
=====
05-14 14:23:34 - [INFO] processing message WEAPON_CLOSE_SESSION
05-14 14:23:34 - [INFO] File received and processed successfully

Workspace 1 14 May, Thu 14:39:40 Master Secure Terminal
```