Suspicious traffic

TechmandanCZ

Tato úloha mě naučila zdaleka nejvíce, i když jsem naštěstí věděl co čekat díky úloze Cookies na projektu Kyberchod (složka AppData, je potřeba přečíst šifrované cookies).
V Wireshark je vidět různý síťový provoz, ale nejvíce do očí asi bije SMB3, zvláště zašifrovaná část. Tam to určitě musí být.
Rovnou též vidím že se přihlašoval přes HTTP (přidaný sloupec s přihlašovacími údaji ve wiresharku), a později také nacházím FTP provoz kde se uživatel přihlašuje.
Vidím že formát hesla je `james.f0r.<PROT>.<7 cisel>`.
Najdu si jak vytvořit hash pro NetNTLMv2 pro hashcat, a dávám `james.f0r.SMB.<7 cisel>` jako template. A tady se zasekávám na docela delší dobu, než si všimnu že uživatel je james_admin, a pak heslo nacházím hned..

A mám soubor! Akorát .enc. File říká že openssl enc'd with salted password, tak opět zkouším přes různé brute force programy různá hesla - vím že se jedná nejspíše o sqlite databázi, a tak hledám výsledky začínající na SQLite.

Mezitím si prohlížím stažené složky přes FTP, a po delší době si vzpomínám, že bash ukládá historii, a tam je rovnou i heslo. Soubor otevírám v DB Browser for sqlite, a mám vlajku.

A díky tomu že nyní vím že openssl umí šifrovat data přes heslo a není zcela jednoduché dané heslo brute forcenout, vyexportoval jsem si data z bitwarden (správce hesel) a zašifroval si je abych měl zálohu i mimo svoji instanci bitwardenu. Díky!