***PE Blue Team: Windows Foresics 1 (1ster)***

Opdrachten 1 tem 9 waren zeer duidelijk.

Alle gegeven documentatie doorgelezen alvorens de oefeningen gemaakt te hebben.

De antwoorden van alle oefeningen staan in de tekst en de printscreens van de documentatie.

De antwoorden op al deze vragen kun je vinden in de documentatie over het desbetreffende onderwerp.  
Geen problemen tegengekomen.

Task10:

De notitie bij de eerste oefening zegt dat we registry explorer moeten gebruiken dus hebben we alle opdrachten opgelost in de registry explorer (gegeven in de vm van TryHackMe)

10.1:

De hint zegt dat we de SAM hive moeten gebruiken om users terug te vinden en dat accounts startend met 10xx user accounts zijn.

De file “SAM” geladen in registry explorer (te vinden in de triage map onder C\Windows\Systems32\config.) -> Dit hebben we geleerd in het deel “Accessing registry hives offline”.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Probleem:

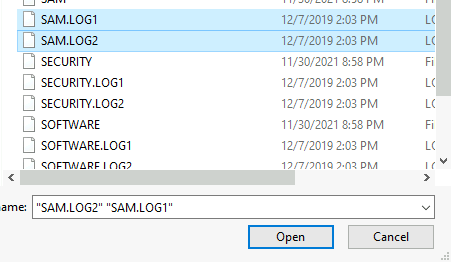
1. Tijdens het inlezen van de SAM file krijgen we een waarschuwing van diry hive.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Oplossing:

1. Omdat we een clean hive willen hebben laden we de log files in ipv de algemene SAM hive. De LOG1 en LOG2 files van SAM ingeladen om te vergelijken en een “clean” bestand opgeslagen om dit dan te gebruiken.

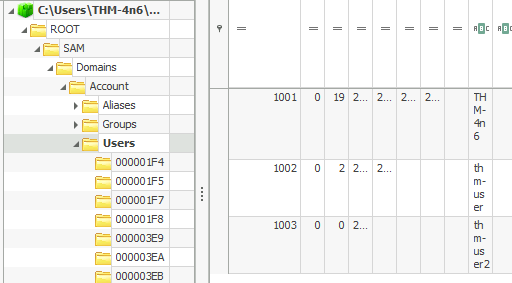


Afbeelding met tekst

Automatisch gegenereerde beschrijving

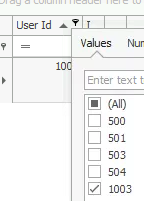
Daarna file opgeslagen op de desktop als SAM\_clean.

De userID’s opgezocht in users.



10.2:

In de kolom last login time “empty” geselecteerd en daar de user met een id 10XX gezocht.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tafel

Automatisch gegenereerde beschrijving

10.3:

In de kolom “Password hint” staat count bij deze user, dus de hint is count.

Afbeelding met tafel

Automatisch gegenereerde beschrijving

10.4:

Probleem:

1. Locatie vinden in Registry Explorer waar de info van “Changedlog.txt” staat.
2. NTUSER.DAT was coprimised

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Oplossing:

1. Na opzoek werk in het deel van “Usage of knowledge of files/folders” hebben we de NTUSER.DAT file ingeladen van het admin account (THM-4n6) en daarna de folder “recent docs” geselecteerd die we gevonden hebben in Software\Microsoft\Windows\CurrentVersion\Explorer\

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1. De LOG1 en LOG2 files van NTUSER genomen om te vergelijken

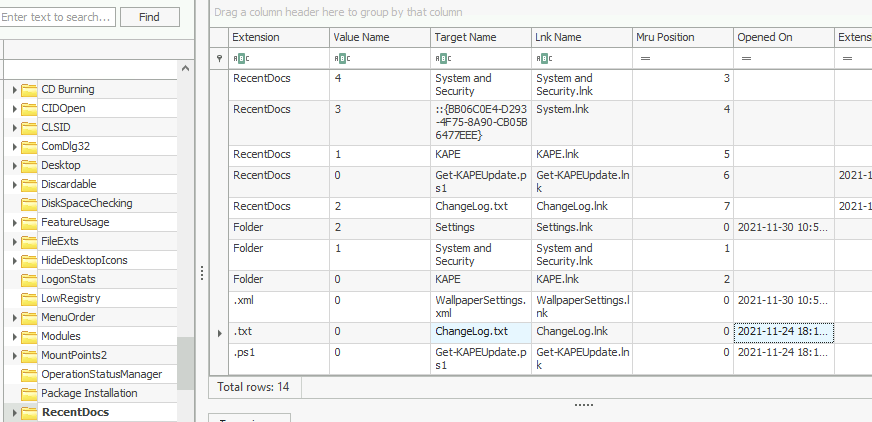
Afbeelding met tafel

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Daarna file opgeslagen op de desktop als NTUSER.DAT\_clean.



10.5:

Na opzoekwerk in het deel van “Evidence of Execution” stond dat UserAssist een log bijhoudt van gestarte applicaties.

Afbeelding met tekst

Automatisch gegenereerde beschrijving  
We hebben we elke entry in software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\ doorzocht naar een path met python-3.8.2

Afbeelding met tafel

Automatisch gegenereerde beschrijving

10.6:

Probleem:

1. Waar kunnen we de info van geconnecteerde usb toestellen vinden?
2. De datum en uur van de laatste connectie van de gevonden USB was niet gegeven in de map Windows portable devices

Oplossing:

1. Deze info hebben we gevonden in het deel van “External Devices/USB device forensics”

We hebben dan de SOFTWARE hive van systems32 config file “Software” geladen om hier “windows portable devices” te raadplegen onder de map Microsoft.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Dit gaf ons enkel het GUID van de USB die we zochten.

Afbeelding met tafel

Automatisch gegenereerde beschrijving

1. Dit hebben we gevonden door de SYSTEM hive te laden om te gaan kijken onder USB en USBSTOR.

Deze info hebben we ook gevonden in het deel van “External Devices/USB device forensics”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hier stond de GUID van de USB die we nodig hebben met een kolom “last connected”

